AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

DOE MANAGEMENT AND OVERSIGHT OF ITS NUCLEAR WEAPONS COMPLEX: LESSONS OF THE Y–12 SECURITY FAILURE

HEARING

BEFORE THE

SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS

OF THE

COMMITTEE ON ENERGY AND COMMERCE

HOUSE OF REPRESENTATIVES

ONE HUNDRED THIRTEENTH CONGRESS

FIRST SESSION

MARCH 13, 2013

Serial No. 113–13

Printed for the use of the Committee on Energy and Commerce

energycommerce.house.gov

U.S. GOVERNMENT PRINTING OFFICE

80–292 WASHINGTON : 2013

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON ENERGY AND COMMERCE

FRED UPTON, Michigan
Chairman

RALPH M. HALL, Texas
JOE BARTON, Texas
Chairman Emeritus
ED WHITFIELD, Kentucky
JOHN SHIMKUS, Illinois
JOSEPH R. PITTS, Pennsylvania
GREG WALDEN, Oregon
LEE TERRY, Nebraska
MIKE ROGERS, Michigan
TIM MURPHY, Pennsylvania
MICHAEL C. BURGESS, Texas
MARSHA BLACKBURN, Tennessee
Vice Chairman
PHIL GINGREY, Georgia
STEVE SCALISE, Louisiana
ROBERT E. LATTA, Ohio
CATHY MCMORRIS RODGERS, Washington
GREGG HARPER, Mississippi
LEONARD LANCE, New Jersey
BILL CASSIDY, Louisiana
BRETT GUTHRIE, Kentucky
PETE OLSON, Texas
DAVID B. MCKINLEY, West Virginia
CORY GARDNER, Colorado
MIKE POMPEO, Kansas
ADAM KINZINGER, Illinois
H. MORGAN GRIFFITH, Virginia
GUS M. BILIRAKIS, Florida
BILL JOHNSON, Missouri
BILLY LONG, Missouri
RENEE L. ELLMERS, North Carolina

HENRY A. WAXMAN, California
Ranking Member
JOHN D. DINGELL, Michigan
Chairman Emeritus
EDWARD J. MARKEY, Massachusetts
FRANK PALLONE, JR., New Jersey
BOBBY L. RUSH, Illinois
ANNA G. ESHOO, California
ELIOT L. ENGEL, New York
GENE GREEN, Texas
DIANA DEGETTE, Colorado
LOIS CAPPS, California
MICHAEL F. DOYLE, Pennsylvania
JANICE D. SCHAKOWSKY, Illinois
ANTHONY D. WEINER, New York
JIM MATHESON, Utah
G.K. BUTTERFIELD, North Carolina
JOHN BARROW, Georgia
DORIS O. MATSUI, California
DONNA M. CHRISTENSEN, Virgin Islands
KATHY CASTOR, Florida
JOHN P. SARBANES, Maryland
JERRY MCNERNEY, California
BRUCE L. BRALEY, Iowa
PETER WELCH, Vermont
BEN RAY LUJAN, New Mexico
PAUL TONKO, New York

SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS

TIM MURPHY, Pennsylvania
Chairman

MICHAEL C. BURGESS, Texas
Vice Chairman
MARSHA BLACKBURN, Tennessee
PHIL GINGREY, Georgia
STEVE SCALISE, Louisiana
GREGG HARPER, Mississippi
PETE OLSON, Texas
CORY GARDNER, Colorado
H. MORGAN GRIFFITH, Virginia
BILL JOHNSON, Ohio
BILLY LONG, Missouri
RENEE L. ELLMERS, North Carolina
JOE BARTON, Texas
FRED UPTON, Michigan *(ex officio)*

DIANA DEGETTE, Colorado
Ranking Member
BRUCE L. BRALEY, Iowa
BEN RAY LUJAN, New Mexico
EDWARD J. MARKEY, Massachusetts
JANICE D. SCHAKOWSKY, Illinois
G.K. BUTTERFIELD, North Carolina
KATHY CASTOR, Florida
PETER WELCH, Vermont
PAUL TONKO, New York
GENE GREEN, Texas
JOHN D. DINGELL, Michigan
HENRY A. WAXMAN, California *(ex officio)*

CONTENTS

	Page
Hon. Tim Murphy, a Representative in Congress from the Commonwealth of Pennsylvania, opening statement	1
Prepared statement	3
Hon. Diana DeGette, a Representative in Congress from the state of Colorado, opening statement	4
Hon. Fred Upton, a Representative in Congress from the state of Michigan, opening statement	5
Prepared statement	6
Hon. Michael C. Burgess, a Representative in Congress from the State of Texas, opening statement	7
Hon. Henry A. Waxman, a Representative in Congress from the State of California, opening statement	8

WITNESSES

Sandra E. Finan, Brigadier General, USAF, Commander, Air Force Nuclear Weapons Center and Former Acting Chairman of Defense Nuclear Security, National Nuclear Security Administration (NNSA)	9
Prepared statement	11
Daniel B. Poneman, Deputy Secretary, U.S. Department of Energy, Accompanied by Neile L. Miller, Acting Undersecretary for Nuclear Security and Acting Administrator, NNSA	27
Prepared statement	29
Answers to submitted questions	181
Richard A. Meserve, President, Carnegie Institution for Science	56
Prepared statement	58
Answers to submitted questions	191
C. Donald Alston, Major General, USAF (Retired)	57
Prepared statement	58
Answers to submitted questions	191
David C. Trimble, Director, Natural Resources and Environment Team, Government Accountability Office	83
Prepared statement	85
Answers to submitted questions	193

SUBMITTED MATERIAL

Document binder	116

DOE MANAGEMENT AND OVERSIGHT OF ITS NUCLEAR WEAPONS COMPLEX: LESSONS OF THE Y–12 SECURITY FAILURE

WEDNESDAY, MARCH 13, 2013

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS,
COMMITTEE ON ENERGY AND COMMERCE,
Washington, DC.

The subcommittee met, pursuant to call, at 10:10 a.m., in room 2322 of the Rayburn House Office Building, Hon. Tim Murphy (chairman of the subcommittee) presiding.

Members present: Representatives Murphy, Burgess, Harper, Gardner, Johnson, Barton, Upton (ex officio), DeGette, Braley, Luján, Tonko, Green, and Waxman (ex officio).

Staff present: Carl Anderson, Counsel, Oversight; Charlotte Baker, Press Secretary; Mike Bloomquist, General Counsel; Annie Caputo, Professional Staff Member; Karen Christian, Counsel, Oversight; Andy Duberstein, Deputy Press Secretary; Kirby Howard, Legislative Clerk; Peter Kielty, Deputy General Counsel; Peter Spencer, Professional Staff Member, Oversight; Tiffany Benjamin, Democratic Senior Counsel; Brian Cohen, Democratic Staff Director, Oversight and Investigations, and Senior Policy Advisor; Elizabeth Letter, Democratic Assistant Press Secretary; and Stephen Salsbury, Democratic Special Assistant.

OPENING STATEMENT OF HON. TIM MURPHY, A REPRESENTATIVE IN CONGRESS FROM THE COMMONWEALTH OF PENNSYLVANIA

Mr. MURPHY. Good morning. We convene this hearing to continue the committee's examination of Department of Energy's management and oversight of its nuclear weapons complex, three national weapons laboratories and five production and testing facilities. These eight sites are responsible for the stewardship of our Nation's nuclear weapons stockpile.

DOE, through its National Nuclear Security Administration, or NNSA, spends billions of dollars each year performing hazardous operations to maintain and secure nuclear weapons and weapons materials. This work is performed by contractors at the Department's nuclear weapons sites under the supervision of federal officials and requires strict adherence to strong safety standards. The supremely sensitive nature of the materials and technologies also requires the Department to ensure an extraordinary level of security to safeguard these nuclear sites and operations.

Our attention today will focus mainly on the lessons for the Department from the security and oversight failures that occurred last summer at the Y–12 National Security Complex, in Oak Ridge, Tennessee, and what DOE is doing to address these lessons.

At its hearing this past September, this subcommittee began to examine preliminary information about the failures at Y–12. We learned how these failures allowed three protestors at around 4:20 a.m. one morning last July to penetrate security fences and detection systems and deface the walls of the facility storing highly enriched uranium. We learned about inexcusable maintenance problems and compensatory security measures to work around broken equipment and chronic false alarms. We learned about the inadequate response by the protective guard force. And most to the point of our hearing today, we learned about the failure of contractor governance and federal oversight to identify and correct the multiple early indicators of Y–12's security, maintenance, and communications systems breakdowns.

The DOE Inspector General's testimony at that hearing revealed that federal site officials did not do anything to address security maintenance backlogs because NNSA's contractor governance system meant "they could no longer intervene." This perhaps is the most incomprehensible aspect of this troubling situation. It appears that, due to a "hands off" federal contracting policy, we had ineffective federal security oversight at Y–12, and potentially at other sites around the complex.

Information produced since September confirms that a strong oversight approach to security has not been paramount at DOE, particularly since the Department instituted certain reforms to its oversight in 2009 and 2010. The stated purpose of these reforms was to give contractors flexibility to tailor and implement safety and security programs "without excessive federal oversight or overly prescriptive departmental requirements." Whatever the intent, the reforms in practice were interpreted by federal site officials to mean they couldn't intervene when security problems arose.

We will discuss today the findings of a revealing Task Force assessment, which was commissioned in response to Y–12 and released to the administrator in November. Led by Air Force Brigadier General Sandra Finan, who will testify on the first panel this morning, the Task Force found that issues at Y–12 were part of a larger pattern of deficiencies in NNSA's security-related functions and activities across board. Notably, the Task Force found no clear lines of accountability at NNSA, and broken security policy process, an "eyes on, hands off" governance approach that weakened federal oversight, and a federal organization "incapable of performing effective security performance assessment" of the contractors operating the sites.

We will hear testimony from GAO on our second panel that many of these deficiencies are identical to those identified at NNSA 10 years ago. It appears the Department instituted reforms that actually may have exacerbated the deficiencies, turning "eyes on, hands off" into eyes closed, hands off.

Deputy Secretary Poneman and acting NNSA Administrator Miller I trust will explain to us today how and when the agency will implement the Task Force's recommendations and exactly how they

will communicate clear and appropriate priorities for safety and security in their governance of the sites. Let me welcome you both, and General Finan.

Our second panel provides broader perspective on security culture at the Department. Along with GAO, we will hear from General Donald Alston and former NRC Chairman Richard Meserve, two of three contributors to an analysis requested by the Secretary of Energy about the physical security structure at the DOE.

The experience and perspective of these witnesses should help us to put the security deficiencies in the broader context of the oversight and management challenges confronting DOE. In the end we should identify a path forward for the Department to ensure strong oversight and zero tolerance for failures. The risks to millions of people, and indeed geopolitics are too important for anything less.

[The prepared statement of Mr. Murphy follows:]

PREPARED STATEMENT OF HON. TIM MURPHY

Good Morning. We convene this hearing to continue the Committee's examination of the Department of Energy's management and oversight of its nuclear weapons complex—three national weapons laboratories and five production and testing facilities. These eight sites are responsible for the stewardship of our nation's nuclear weapons stockpile.

DOE, through its National Nuclear Security Administration (or NNSA), spends billions of dollars each year performing hazardous operations to maintain and secure nuclear weapons and weapons materials. This work is performed by contractors at the Department's nuclear weapons sites under the supervision of federal officials and requires strict adherence to strong safety standards. The supremely sensitive nature of the materials and technologies also requires the Department to ensure an extraordinary level of security to safeguard these nuclear sites and operations.

Our attention today will focus mainly on the lessons for the Department from the security and oversight failures that occurred last summer at the Y–12 National Security Complex, in Oak Ridge Tennessee—and what DOE is doing to address these lessons.

At its hearing this past September, this Subcommittee began to examine preliminary information about the failures at Y–12. We learned how these failures allowed three protestors at around 4:20 a.m. one morning last July to penetrate security fences and detection systems and deface the walls of the facility storing highly enriched uranium.

We learned about inexcusable maintenance problems and "compensatory" security measures to work around broken equipment and chronic false alarms. We learned about the inadequate response by the protective guard force.

And most to the point of our hearing today, we learned about the failure of contractor governance and Federal oversight to identify and correct the multiple early indicators of Y–12's security, maintenance, and communications systems breakdowns.

The DOE Inspector General's testimony at that hearing revealed that federal site officials did not do anything to address security maintenance backlogs because NNSA's contractor governance system meant "they could no longer intervene." This perhaps is the most incomprehensible aspect of this troubling situation. It appears that, due to a "hands off" federal contracting policy, we had ineffective federal security oversight at Y–12—and potentially at other sites around the complex.

Information produced since September confirms that a strong oversight approach to security has not been paramount at DOE, particularly since the Department instituted certain reforms to its oversight in 2009 and 2010. The stated purpose of these reforms was to give contractors flexibility to tailor and implement safety and security programs "without excessive federal oversight or overly prescriptive departmental requirements." Whatever the intent, the reforms in practice were interpreted by federal site officials to mean they couldn't intervene when security problems arose.

We will discuss today the findings of a revealing Task Force assessment, which was commissioned in response to Y–12 and released to the Administrator in November. Led by Air Force Brigadier General Sandra Finan, who will testify on the first panel this morning, the Task Force found that issues at Y–12 were part of a larger

pattern of deficiencies in NNSA's security-related functions and activities across board.

Notably, the Task Force found no clear lines of accountability at NNSA, a broken security policy process, an "eyes on, hands off" governance approach that weakened Federal oversight, and a federal organization "incapable of performing effective security performance assessment" of the contractors operating the sites.

We will hear testimony from GAO on our second panel that many of these deficiencies are identical to those identified at NNSA ten years ago. It appears the Department instituted reforms that actually may have exacerbated the deficiencies—turning "eyes on, hands off" into eyes closed, hands off.

Deputy Secretary Poneman and acting NNSA Administrator Miller I trust will explain to us today how and when the agency will implement the Task Force's recommendations and exactly how they will communicate clear and appropriate priorities for safety and security in their governance of the sites. Let me welcome you both, and General Finan.

Our second panel provides broader perspective on security culture at the Department. Along with GAO, we will hear from General Donald Alston and former NRC Chairman Richard Meserve, two of three contributors to an analysis requested by the Secretary of Energy about the physical security structure at the DOE.

The experience and perspective of these witnesses should help us to put the security deficiencies in the broader context of the oversight and management challenges confronting DOE. In the end we should identify a path forward for the Department to ensure strong oversight and zero tolerance for failures. The risks to millions of people, and indeed geopolitics are too important for anything less.

# # #

Mr. MURPHY. I would now like to recognize Ranking Member Diana DeGette for her opening statement.

OPENING STATEMENT OF HON. DIANA DEGETTE, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF COLORADO

Ms. DEGETTE. Thank you, Mr. Chairman.

Mr. Chairman, as you said, a little over 7 months ago, an 82-year-old nun and two middle age men breached the security perimeter surrounding the highly-enriched uranium facility at the Y–12 National Security Complex in Oak Ridge, Tennessee. In the wake of that incident, this committee had a hearing toward exactly how such an absurd and dangerous breach of security could happen. Today, I want to thank you for having this follow-up hearing to learn what has happened to address the security breakdowns that resulted in the breach, and to make sure that something like that never happens again.

I want to thank you, Mr. Chairman, for continuing our long-standing bipartisan interest in this subcommittee in ensuring that our nuclear facilities are safe and secure.

Our past oversight over the nuclear complex has made a significant difference, raising standards for worker safety, ensuring lab safety, ensuring security standards remain accountable to those who work within the labs and who live nearby, and forcing NNSA to make significant changes when things go awry. But I got to tell you, as I have told you before, both on and off the record, every few years we go through this same thing. There is an incident, there is an aggressive response from NNSA, time passes without an incident, and everybody begins to relax. Labs start to complain about overly burdensome paperwork and oversight. In response, expectations and rules are relaxed, and then, of course, without fail, another incident occurs. I am tired of this pattern and we should all

be tired of this pattern, because it really does affect our national security.

Today, I am hoping to hear how NNSA and DOE have responded to last year's call to action, not just at Y–12, but across the NNSA complex. But more importantly, I want to hear what they are doing to ensure that we don't have to have any more hearings about security breaches or safety incidents at these sites. I guess my view is, it is time to break this pattern.

I want to commend the agencies for acting promptly to address the issues exposed at Y–12 in the wake of the July 28 breach. However, I continue to be deeply concerned about oversight within NNSA. Last month, GAO again released its high risk list, identifying agencies and program areas that are at high risk due their vulnerabilities to fraud, waste, abuse, and mismanagement. Just as it has been since 1990, contract management at NNSA is on this list. Assessments conducted after last year's security breach show that NNSA dubious honor is well-deserved. A February, 2013, DOE Inspector General report described a "eyes on, hands off" approach to contractor oversight, meaning federal employees felt they could monitor but not intervene in contractor activities, even if they suspected an issue. Recent assessments conducted by DOE's Office of Health, Safety, and Security showed contractor communication problems, both between different contractors at the Y–12 site, and between the contractor and federal employees at Y–12, and other independent experts observed a Y–12 culture that completely failed to adequately focus on security.

As terror effects become more real, and as our enemies become more sophisticated, we just can't afford to take this "eyes on, hands off" approach to security. Tens of thousands of people work at these labs and facilities, and we owe it to them and to the communities around the facilities and the American people to ensure that they are safe and secure. To do that, we have got to closely examine and monitor the nuclear complex, promote transparency when it comes to how DOE and NNSA are using their resources, and demand accountability from everybody involved. We have to insist that standards are simply never relaxed because people don't like filling out paperwork. In short, we have to demand more.

There has been no shortage of assessments of what should be done for the complex, and in the coming months, I am sure we can expect more of these. As we move forward, we have to continue to make sure that DOE and NNSA are keeping nuclear safe sites safe and adapting and responding to the ever-changing security challenges at the nuclear complex.

So Mr. Chairman, I am happy that you are continuing the grant tradition of this subcommittee in oversight of DOE and NNSA, and I look forward to working with you as we move along in the future. I yield back.

Mr. MURPHY. I thank the Congresswoman from Colorado.

I now recognize the chairman of the full committee, Mr. Upton, for an opening statement.

OPENING STATEMENT OF HON. FRED UPTON, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF MICHIGAN

Mr. UPTON. Well thank you, Mr. Chairman.

Today's hearing represents another important step in this committee's ongoing oversight to ensure that the Department of Energy's management of nuclear security enterprise can successfully protect taxpayer dollars, ensure public health and worker safety, and in fact, safeguard our national security assets. We know from our past work, as well as from the recent and very troubling security failures at Y–12, that management reform is necessary to ensure safe and secure operations. The challenge has been learning the right lesson from past failures, and then successfully implementing the right fixes.

Time and again over the last 14 years, we have witnessed dramatic failures in safety and security, as well as taxpayer waste across the nuclear complex. Despite that poor track record, in '09 DOE proposed increased economy and less oversight as the appropriate corrective actions. We know, though, from past experiences and the Y–12 breach that strong and consistent federal management bolstered by truly independent oversight is, in fact, necessary. DOE leadership must be clear that safety and security come first. They go hand in hand. This is the lesson that we have learned from the civilian nuclear industry. As safety improves, so does performance. Absent an imbedded safety culture, there is erosion of safety practices, leading to outages, delays, and other operational impacts. The same is true for security.

The Y–12 security breach demonstrated not only a failure at the site, but also a failure of DOE and NNSA management. We can trace some of that failure to the initiative launched by DOE leadership 3 to 4 years ago to rely more on contractor's self-assessments and define success as productivity gained. Secretary Chu himself wanted DOE to be viewed as a "partner and asset," his words for the contractors, sending the signal that oversight of these contractors would not be a priority. Members on this committee warned the Secretary in 2010 that such initiatives, however well-intentioned, were misinterpreting the lessons and the past and could, in fact, backfire, and that track record speaks for itself.

As this committee, with oversight responsibility for DOE, we must ensure that current and future DOE leadership learns the right lessons. That starts today when we hear about the plans to fix and sustain improvements in safety and security oversight.

I yield the balance of my time to Dr. Burgess.

[The prepared statement of Mr. Upton follows:]

PREPARED STATEMENT OF HON. CHAIRMAN FRED UPTON

Today's hearing represents another important step in this committee's ongoing oversight to ensure the Department of Energy's management of the nuclear security enterprise can successfully protect taxpayer dollars, ensure public health and worker safety, and safeguard our national security assets.

We know from both our past work, as well as from the recent and very troubling security failures at Y–12, that management reform is necessary to ensure safe and secure operations. The challenge has been learning the right lessons from past failures and then successfully implementing the right fixes.

Time and again over the past 14 years, we have witnessed dramatic failures in safety, security, and taxpayer waste across the nuclear complex. Despite this poor track record, in 2009 DOE proposed increased autonomy and less oversight as the appropriate corrective actions.

We know, though, from past experience and the Y–12 breach that strong and consistent federal management, bolstered by truly independent oversight, is necessary. DOE leadership must be clear that safety and security come first.

Safety and performance go hand-in-hand. This is the lesson we've learned from the civilian nuclear industry. As safety improves, so does performance. Absent an embedded safety culture, there is erosion of safety practices, leading to outages, delays, and other operational impacts. The same is true for security.

The Y–12 security breach demonstrated not only a failure at the site, but also a failure of DOE and NNSA management. We can trace some of this failure to the initiatives launched by DOE leadership three and four years ago to rely more on contractor self-assessments, to reduce "burdensome" oversight, and to define success as productivity gains. Secretary Chu himself wanted DOE to be viewed as a "partner and asset" for the contractors, sending a signal that oversight of these contractors would not be a priority.

Members on this committee warned the Secretary in 2010 that such initiatives—however well-intentioned—were misinterpreting the lessons of the past and could backfire. DOE's track record speaks for itself.

As the committee with oversight responsibility for DOE, we must ensure that current and future DOE leadership learn the right lessons. This will start today, when DOE/NNSA explains that it has serious plans for fixing and sustaining improvemes in safety and security oversight.

# # #

OPENING STATEMENT OF HON. MICHAEL C. BURGESS, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF TEXAS

Mr. BURGESS. I thank the chairman of the full committee—chairman of the subcommittee for calling this important hearing. This is an important follow-up on the committee's work in the last Congress into the astonishing security lapses that occurred at one of our most important, and purportedly most secure nuclear weapons facilities in the country.

You know, you look at the continuum, the range of failure and it goes from totally unacceptable to an abject failure, and this is at one of our country's most important facilities that stores highly enriched uranium for our defenses and for our national security. At last September's hearing, I voiced my concern over the lack of accountability. We need to know who at Department of Energy was held accountable. Who lost their job? Who lost their job because of this epic failure of security and oversight?

Now, General Finan's task force, I think, has put it very succinctly that there is a pervasive culture of tolerating the intolerable and accepting the unacceptable. I fear that statement has really become the operational motto of the Executive Branch, where failure after failure is met with a shrug and not much more. Had this incident been perpetrated by someone with more sinister motives, the break-in could have had catastrophic results for that region and for our Nation. So I continue to be concerned that our security at our Nation's most critical facilities is not being given the priority that it deserves.

Chairman Murphy and I met with General Finan, and I thank you, General, for taking the time for that meeting—this was a month ago—to discuss some of the observations that her task force has made in the security lapses and the oversight failures at NNSA. So certainly, we look forward to hearing from you this morning as to where the NNSA stands in its oversight of these facilities.

This investigation is a prime example of the good work that this committee can do when it works in a bipartisan manner. The security of our Nation's weapons facilities is not an issue that divides or should divide along party lines. We are all in favor of safe, secure areas where our nuclear stockpiles can be held, ready to protect our Nation, and safe from predators.

With that, Mr. Chairman, I will yield back.

Mr. MURPHY. Thank the gentleman. I will now recognize for 5 minutes the ranking member of the full committee, Mr. Waxman.

OPENING STATEMENT OF HON. HENRY A. WAXMAN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF CALIFORNIA

Mr. WAXMAN. Thank you, Mr. Chairman, for recognizing me and for holding this hearing.

The Y–12 incident was embarrassing for DOE and NNSA, the National Nuclear Security Administration. It exposed serious issues within the security organization at NNSA. I appreciate our witnesses being here today, and I hope they will help us identify and address these concerns.

The security concerns we will hear about today must be addressed. We cannot let our nuclear facilities become targets for our foreign enemies and terrorists. We need to invest in the safety and security of these facilities, both financially and by ensuring they have a culture that is focused on keeping our nuclear legacy materials and the people who work with them safe and secure.

I appreciate DOE's actions in the wake of the Y–12 incident. The Department has taken this incident seriously and developed a thoughtful approach to addressing concerns that have been identified, but there is still more work left to be done. DOE needs to ensure that it exercises strong oversight over both its contractors and its federal employees at NNSA sites, and as noted by General Finan today, DOE needs to ensure that there is a clear line of authority from the Secretary down to the contractor, security guards at every site.

Over the years, many people have advocated many different structures for NNSA, but the assessments made after the Y–12 incident show that the problem is not too much DOE efforts oversight, it is too little. The problem is that contractors didn't take their responsibilities to the government or their workers seriously. The federal employees failed to exercise appropriate authority over the contractor counterparts, and that NNSA's culture didn't adequately focus on security.

These problems can be resolved by effective oversight by DOE by requiring that contractors become accountable and transparent, and by ensuring that the federal officials who oversee these contractors take a hands on approach to oversight.

In the past year, some have suggested that NNSA needs more autonomy. In fact, last year's House-passed National Defense Authorization Act included language stripping DOE's authority over some NNSA sites. Given what we have seen in the last 7 months, that approach makes absolutely no sense. The Y–12 breach made it abundantly clear that NNSA is not doing enough on its own. All the findings and recommendations that have come from inde-

pendent evaluators of the Y–12 breach, including NNSA's own task force, show that NNSA needs more oversight, not less. NNSA sites house some of our most dangerous nuclear assets. We need vigorous oversight by DOE to ensure that these nuclear materials are appropriately protected.

Mr. Chairman, again, thank you for holding this hearing. I look forward to more opportunities to check in on NNSA's progress. I yield back the balance of my time.

Mr. MURPHY. The vice chairman yields back, and now we will go over our witnesses today.

With us today is Brigadier General, United States Air Force, Sandra Finan. I hope I am pronouncing that right. I believe I am, right? Thank you for being here. She is the Commander of the Air Force Nuclear Weapons Center and former Acting Chief of Defense Nuclear Security, National Nuclear Security Administration.

Also joining her is Daniel B. Poneman, Deputy Secretary, U.S. Department of Energy. Thank you so much for being with us today, sir, and also accompanied by Neile Miller, the Acting Administrator of NNSA. I hope I have all the title correct.

As you know, the testimony you are about to give is subject to Title XVIII, Section 1001 of the United States Code. When holding an investigative hearing, this committee has a practice of taking testimony under oath. Do you have any objections to testifying under oath?

The chair then advises you that under the rules of the House and rules of the committee, you are entitled to be advised by counsel, if you desire to be advised by counsel during your testimony today. OK, they all say no.

Then in that case, if you would please rise and raise your right hand, and I will swear you in.

[Witnesses sworn.]

Mr. MURPHY. Thank you. Noting for the record that all the witnesses responded in the affirmative, I now call upon each of them to give a 5-minute summary and their written statement.

Starting off with you, General Finan, thank you for being here today.

TESTIMONY OF SANDRA E. FINAN, BRIGADIER GENERAL, USAF, COMMANDER, AIR FORCE NUCLEAR WEAPONS CENTER AND FORMER ACTING CHAIRMAN OF DEFENSE NUCLEAR SECURITY, NATIONAL NUCLEAR SECURITY ADMINISTRATION (NNSA); AND DANIEL B. PONEMAN, DEPUTY SECRETARY, U.S. DEPARTMENT OF ENERGY, ACCOMPANIED BY NEILE L. MILLER, ACTING UNDERSECRETARY FOR NUCLEAR SECURITY AND ACTING ADMINISTRATOR, NNSA

TESTIMONY OF SANDRA E. FINAN

General FINAN. Chairman Murphy, Ranking Member DeGette, distinguished members of the committee, thank you for the opportunity to discuss the study I conducted on the National Nuclear Security Administration's federal security organization——

Mr. MURPHY. Could you pull your mike closer to yourself there, if it is on, too?

General FINAN. Is that better?

Mr. MURPHY. Yes, much better. Thank you.

General FINAN. OK.

Thank you for the opportunity to discuss the study I conducted on the National Nuclear Security Administration's federal security organization and assessment model. Although I am no longer assigned to the NNSA, I am pleased to share our observations based on our 90-day study.

In the aftermath of the July 28, 2012, security incident at the National Nuclear Security Administration's Y–12 National Security Complex, the leadership of the NNSA and the Department of Energy took action to address the security failures at Y–12. The initial information gathered revealed that the issues at Y–12 were part of a larger pattern of security program management deficiencies within NNSA. These security issues prompted the NNSA administrator to commission a task force to analyze the current federal NNSA security organizational structure and security oversight model and recommend possible improvements. The NNSA Administrator directed the Task Force to analyze the current NNSA security organizational structure and recommend possible improvements, and to analyze the current NNSA security oversight model and mechanisms to determine what seams existed and what structures could be implemented to better ensure that the issues are found and fixed before they become problems.

While other reviews were aimed at diagnosing the root causes of the Y–12 event, the NNSA administrator's direction called for this Task Force to focus on the a path forward within the federal NNSA organization. Under my leadership, the task force consisting of NNSA, DOE, and military specialists conducted extensive document reviews and interviewed federal managers and staff as well as a selection of contractor security managers and others across the NNSA security organization. The task force collected and analyzed information, identified issues, and suggested a revised organizational structure and assessment model.

While we highlighted negative aspects of the NNSA security organization and assessment model, the task force found many great people on the NNSA security staffs. They are clearly dedicated, skilled, and hard-working and want to get the security mission done right. Unfortunately, NNSA security personnel have seen themselves thwarted by lack of management support and feel obstructed by some of their peers. Their difficulties were compounded by the absence of a workforce strategy to recruit, retain, and develop a cadre of talented, knowledgeable and experienced security professionals. Thus, it is all the more encouraging that these personnel, almost without exception, genuinely care about doing good work. Their continued strong desire to build a successful security organization is a hopeful sign for the future.

Mr. Chairman, with your permission, I will submit the remainder of my testimony for the record. It contains the findings of the task force.

[The prepared statement of General Finan follows:]

NOT FOR PUBLICATION UNTIL RELEASED BY
HOUSE COMMITTEE ON ENERGY AND COMMERCE
SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS
UNITED STATES HOUSE OF REPRESENTATIVES

PRESENTATION TO THE
HOUSE COMMITTEE ON ENERGY AND COMMERCE
SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS
U.S. HOUSE OF REPRESENTATIVES

SUBJECT: DOE Management and Oversight of Its Nuclear Weapons Complex: Lessons of the Y-12 Security Failure

STATEMENT OF: Brigadier General Sandra E. Finan
Commander, Air Force Nuclear Weapons Center
Based on Previous Position as
Acting Chief of Defense Nuclear Security, NNSA

March 13, 2013

NOT FOR PUBLICATION UNTIL RELEASED BY
HOUSE COMMITTEE ON ENERGY AND COMMERCE
SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS
UNITED STATES HOUSE OF REPRESENTATIVES

Introduction

Chairman Murphy, Ranking Member Degette, distinguished Members of the Committee, thank you for the opportunity to discuss the study I conducted on the National Nuclear Security Administration's (NNSA) federal security organization and assessment model. Although I am no longer assigned to the NNSA, I am pleased to share our observations based on our 90 day study.

In the aftermath of the July 28, 2012 security incident at the National Nuclear Security Administration's Y-12 National Security Complex, the leadership of the NNSA and the Department of Energy (DOE) took action to address the security failures at Y-12. The initial information gathered revealed that issues at Y-12 were part of a larger pattern of security program management deficiencies within the NNSA. These security issues prompted the NNSA Administrator to commission a Task Force to analyze the current Federal NNSA security organizational structure and security oversight model and recommend possible improvements. The NNSA Administrator directed the Task Force to:

- Analyze current NNSA security organizational structure and recommend possible improvements that would improve operational focus, oversight, and culture sustainment.
- Analyze current NNSA security oversight model and mechanisms to determine what seams exist and what structures could be implemented to better ensure that the issues are found and fixed before they become problems.

While other reviews were aimed at diagnosing the root causes of the Y-12 event, the NNSA Administrator's direction called for this Task Force to focus on the "path forward" within the Federal NNSA organization. Under my leadership, the Task Force consisting of NNSA, DOE,

and military specialists conducted extensive document reviews and interviewed Federal managers and staff as well as a selection of contractor security managers and others across the NNSA security organization. The Task Force collected and analyzed information, identified issues, and suggested a revised organizational structure and assessment model.

While we highlighted negative aspects of the NNSA security organization and assessment model, the Task Force found many great people on the NNSA security staffs. They are clearly dedicated, skilled, and hard-working and want to get the security mission done right. Unfortunately, NNSA security personnel have seen themselves thwarted by lack of management support and feel obstructed by some of their peers. Their difficulties were compounded by the absence of a workforce strategy to recruit, retain, and develop a cadre of talented, knowledgeable and experienced security professionals. Thus, it is all the more encouraging that these personnel, almost without exception, genuinely care about doing good work. Their continued strong desire to build a successful security organization is a hopeful sign for the future.

Summary Findings

The Task Force noted significant deficiencies in security organization, oversight, and culture sustainment throughout the NNSA security organizations. In the NNSA security organizations, line management authority was ill-defined and claimed by multiple Federal NNSA organizations. On the one hand, the "Federal field organizations" (federal site offices and the nuclear production office which oversees the management and operating contracts) exercised line management authority over the site security contractors via the contract management structure. On the other hand, the NNSA Headquarters security organization asserted that it also had such authority. Absent clearly defined lines of authority, many individuals asserted authority, while correspondingly few have assigned responsibility. This lack of clear lines of authority

contributed to a widespread practice of decision-making by consensus. When consensus failed, organizational elements acted independently or not at all, which undermined effective implementation of the security program.

The Task Force further noted a significant gap in the current NNSA security organizational structure. At the strategic level the NNSA Headquarters organization had been ineffective and had intervened in field tactical execution. The Federal field organizations had been ineffective in performing their tactical responsibilities for executing the security program and had intervened in strategic matters. Additionally, there had not been a clearly identified operationally-focused organization that bridged the gap between strategic and tactical responsibilities and addressed standardization, field execution, and multi-site analysis.

The Task Force found a weak security performance assessment model. It found that NNSA relied overwhelmingly upon Federal staff simply reviewing contractor-provided data, rather than effectively assessing performance itself. At the same time, misinterpretation of the DOE Safety and Security Reform Plan resulted in less stringent independent oversight of security operations. As a result of numerous interviews, the Task Force also observed that potentially critical management information was not being reported clearly to the appropriate decision makers.

As concerning as these structural and assessment issues might be, the most striking result of this review falls in the area of culture sustainment. It quickly became evident that the Task Force findings closely resembled those presented in numerous prior reports. While NNSA has attempted to correct some identified issues over the years, it has not adequately emphasized effective security mission performance. In recent years, NNSA security leaders have chosen to emphasize security cost containment to the detriment of security program execution. The idea that the requirements for security performance effectiveness are subordinated to cost concerns

had become a prevailing concept in the NNSA security community. This emphasis had become endemic throughout the NNSA security culture, so much so that fundamental facility protection issues such as the protection of operational capabilities came to be regarded as too expensive and therefore "out of bounds" for analysis. The NNSA security culture had focused on fiscal limitations over effective performance. This resulted in an environment in which deficiencies were worked at the margins rather than management addressing core issues.

These issues underscored the critical role of effective leaders. While outside the charter of this Task Force, it must be acknowledged that leadership plays the key role in mission accomplishment. The Task Force recognized that effective leadership may compensate for structural deficiencies within an organization; however, restructuring alone cannot overcome leadership shortcomings. The best assessment model is useless if leaders fail to effectively implement it. Additionally, the assessment model will not be effective unless leaders consistently demand comprehensive, unbiased information. NNSA must take ownership of its history of security failures. Leadership must take bold and enduring actions if this pattern is to be broken.

NNSA Organizational Model

The existing NNSA security organizational structure was convoluted and ineffective. The Task Force observed that lines of authority in virtually every organizational function were divided. The NNSA security function was not well organized or effectively staffed and the NA-70 policy development and implementation process was sub-standard. While the Chief of Defense Nuclear Security is the Cognizant Security Authority (CSA), this responsibility has been unevenly delegated and was open to inconsistent interpretation. Security staffs were responsible to multiple lines of authority and for some functions may not be responsible to anyone. The most

fundamental issues arose from the relationship between NA-70 and the Federal field organizations. NA-70 believed that it had line management authority over the security elements within the Federal field organizations. However, the managers of these field organizations had been formally assigned line management authority. The NNSA Act states that the Chief of Defense Nuclear Security role includes "the development and implementation of security programs". The current interpretation of this provision has been a source of ambiguity due to the mixing of line and staff responsibilities.

Roles and responsibilities were either undefined or not followed. The Task Force identified numerous occasions across the NNSA security organizations where individuals were not allowed to perform assigned duties or assumed roles and responsibilities nominally assigned to others. The confusion of roles and responsibilities was evident in NA-70, within field organizations, and between NA-70 and the field. For example, the approved mission and function statements for the two major divisions within NA-70 have little apparent relationship to the way these offices operated and how they interacted with each other or with the NA-70. Within field organizations, the Task Force noted a number of instances where management precluded staff from performing the assigned roles of their position and/or assigned personnel to unrelated duties. At times, NA-70 acted as a formal line management organization, and asserted responsibilities that were formally assigned to the Federal field security organizations. NA-70 personnel were frequently frustrated by site-level resistance to the programmatic direction they provided and Federal field security managers were often similarly frustrated when NA-70 used its budget authority, its control over the policy process, and other activities to inject itself into what the sites regard as their line management decision-making process.

There were no clear lines of authority. There were overlapping lines of authority and mixed staff and line functions. The CSA function flowed from the NNSA Administrator through the Chief of Defense Nuclear Security to the Federal field organizations. Line management authority went from the NNSA Administrator through the Associate Administrator for Infrastructure and Operations (NA- 00), to the field. However, NA-70 attempted to exert line management authority and provided programmatic guidance directly to the Federal field security managers. While Federal field organizations administer the contracts governing the actual performance of the security mission, NA-70 routinely interacted with the security contractors. Furthermore, NA-70, not the line managers, was the primary executer of the NNSA security budget.

The security policy process was sub-standard. The Task Force identified that there was no clearly articulated or consistently implemented NNSA security policy process. A major concern was the supplanting of DOE Security Orders with generic and less restrictive NNSA policies (NAPs). This appeared to be based on a desire to reduce funding demands through a reduction of requirements. Additionally, the Task Force noted a desire on the part of some NA-70 senior managers to maximize separation from DOE HSS policies and activities. Within NA-70, policy and guidance were issued through a variety of formal and informal mechanisms with erratic distribution. The Task Force identified that some Federal field organizations were inconsistent in their acceptance and application of NA-70 issued policies. Finally, NA-70 policy and guidance tended to be vague resulting in widely differing interpretations by field personnel.

The NNSA Federal security organization was not effectively structured or staffed. While there were clearly strategic (Headquarters) and tactical (Federal field organizations and contractors) levels, there was little indication of an effective operational element with

responsibility for security program functions such as site assistance and standardization of program execution. The Task Force also noted that the Federal field organizations structured their security functions substantially differently. This resulted in a lack of standardization of both organization and execution of the security program. At some sites there was weakening of the security function and reduced senior management attention. There were a number of personnel issues associated with the security professional staff including the lack of a human capital development plan, no career path, and limited mobility. Additionally, the Task Force noted an overreliance on support service contractors who primarily assisted the NA-70 organization.

Federal Assessment Model

The Task Force expended considerable effort attempting to describe, understand and analyze the current assessment model and mechanisms.

The failure to adequately assess security system performance and to clearly and unequivocally report deficiencies to the appropriate senior managers has been identified as a significant contributing cause to the Y-12 security incident. The Task Force focused upon the performance assessment process as implemented by Federal field and Headquarters organizations within NNSA. Although contractor self-assessments were the first-line elements in the security performance assessment process, these were outside the direct scope of the review. Strengthening the contractor self-assessment process is an important objective, but cannot replace a rigorous Federal assessment process.

NNSA did not have an adequate security performance assessment process or capability. The performance assessment capabilities of Federal security organizations within NNSA were

virtually non-existent. Essentially all responsibility for performance assessment was delegated to the Federal field organizations. The current Federal field organizations were typically limited to "shadowing" contractor self-assessments and/or reviewing the reports these self-assessments generated. Moreover, there was a tendency on the part of some field Federal staff to adopt the role of defending "their" contractors rather than attempting to objectively assess contractor performance. At the Headquarters level, the NA-70 performance assessment function had only three full-time Federal staff members. The Task Force noted that the NA-70 assessment process was largely confined to the review of submitted paperwork. The result was that there was no NNSA Federal organization capable of performing effective security performance assessment.

The "systems-based" assessment model as implemented was ineffective for security. Misinterpretation, and/or misapplication of the DOE Safety and Security Reform Plan, dated March 16, 2010, resulted in a weakened Federal security assessment program. In particular, this document stated: "Security Performance: Contractors are provided the flexibility to tailor and implement security programs in light of their situation and to develop corresponding risk- and performance-based protection strategies without excessive Federal oversight or overly-prescriptive Departmental requirements." This guidance was further expanded upon and eventually articulated in NAP-21, Transformation Governance and Oversight Initiative. The belief arose that 'eyes on, hands off' precluded Federal security staff from conducting performance-based assessments of contractors. As a result, most Federal assessment was based on paperwork generated by the contractor. This paper-based system of assessment, without sufficient performance verification, was inadequate for effective evaluation of security operations.

NNSA had no clear and consistent performance baseline for security program implementation. A performance baseline, set forth in detailed standards and criteria, is the keystone of an effective security program. Precisely articulated standards and criteria further provide an objective foundation for performance assessment. NNSA did not have the standards or criteria necessary to effectively measure security program performance. The absence of such standards and criteria diminished the ability to identify potentially significant performance deficiencies. The Task Force noted that the lack of standards and criteria had been coupled with the widespread notion that contractors must only be told "what" the mission is, not "how" the mission is to be accomplished. While this approach may be appropriate in other areas, it was ineffective as applied to security programs. Therefore, security tasks were not necessarily performed in a manner consistent with NNSA security requirements.

The current assessment process was biased against criticism. The Task Force noted a distinct bias against finding and stating performance criticisms. The NNSA Federal assessment relies heavily on contractor self-assessment. While an important and useful tool, contractor self-assessments tend to be insufficiently objective. The primary Federal assessment role was performed by field staff. Long-term geographic proximity to site contractors can compromise the objectivity of these Federal assessors. Moreover, the intermingling of management and assessment roles within Federal field organizations can also contribute to less objective assessment. The NA-70 Headquarters performance assessment process, being paper-based, could not validate the information submitted. Information provided to the Task Force suggested that in some instances information considered to be unfavorable was being "watered down" or obscured. Furthermore, information was presented that indicate differing opinions were being

suppressed by some senior managers in the field and at Headquarters. As a result, NNSA senior leadership may not have received all information needed to make quality decisions.

Recommended Organizational Structure

Recommend an organizational structure that separates the line function for executing the security mission from the Headquarters staff function. Additionally, create an operational-level organization that focuses on security implementation and standardization. Distinct roles and responsibilities should be associated with tactical, operational, and strategic-level security functions. Tactical execution of contract administration occurs at the Federal field organizations. Operational implementation and standardization of operations across the security program occurs at the NA-00 level. Strategic-level policy guidance, requirements determination, and performance assessment occur in Headquarters NNSA, NA-70.

In order to clarify the line of authority, CSA must flow from the NNSA Administrator, through the head of the NA-00, to the Federal field managers, and finally to the designated CSA at field sites, with no re-delegations authorized to non-Federal individuals. This authority should follow the same path as the line authority. The asserted security line management tie between the Chief of Defense Nuclear Security and the security managers in the field should be terminated in order to ensure a single, clear line of authority.

In terms of clarifying line and staff functions, the current NA-70 organization needs to be restructured so that it serves solely as a staff organization at the strategic level. Specific alignment within the divisions can be varied. The most important change in NA-70 is the stand-up of the Performance Assessment Division -- a new function responsible for assessment of

contractor and Federal field organization performance. This is the entity that the Chief of Defense Nuclear Security would use to verify that security programs are properly implemented.

A new security operations organizational level needs to be stood up within the NA-00 structure. The responsibilities of this office are to ensure that the policies and guidance provided by the NA-70 staff are executed in the field. It will also ensure standardization of security procedures across the field locations as well as provide field assistance, and a conduit for field concerns to be surfaced to the NA-70 staff.

Resource planning and budgeting, and project management responsibilities will be realigned from NA-70 to the new operational-level organization. This establishes a clear linkage between budget formulation and mission execution and establishes an equally clear boundary between budget considerations and the formulation of requirements. An expanded intelligence/counterintelligence liaison is intended to ensure that Federal security managers get needed information and have appropriate ties to law enforcement and intelligence-related agencies.

At the tactical level in the field, the multiple lines of authority are eliminated and direction will come from a single line of authority. All authorities will run through the Federal field organization manager to the appropriate security manager. The Federal field organization scope of duties will include primary contract administrative functions--including reviews of contractor reports, analysis, security plans, and other required documentation; partnering with the executing contractor; remaining knowledgeable and up-to-date on the content, operations, and effectiveness of the contractor's security implementation; alerting management of all concerns related to contractor execution of the security mission.

This organizational structure will help define and clarify roles and responsibilities and facilitate a strong mission focus. It divides resourcing from requirements determination in order to ensure that requirements are appropriately stated, weighed against budget resources and decisions made on accepting risks at the appropriate level. It provides a single line of authority to those operating in the field and maintains an appropriate span of control.

Recommended Assessment Model

Recommend a three-tiered assessment process that strengthens the role of Federal security assessment within NNSA without diminishing the legitimate need for contractors to maintain their own self-assessment capabilities.

The contractor self-assessment process continues as a first tier in the overall assessment process. The primary audience for the contractor self-assessments should be the contractor security managers themselves. However, the self-assessments should follow a consistent, program-wide format, and be made available for review at all higher levels of management. Contractors should be required to identify, report, and resolve security issues--sanctions should come when a higher level assessment uncovers problems that the contractor self-assessments fail to identify or properly address. Even when an issue is readily resolved and corrective actions are immediate, a finding should be issued and the corrective action recorded. Failure to do so inevitably hides potential negative trends. Contractor self-assessments should involve active performance testing rather than simply relying on work observation and document review--effective security performance can only be evaluated through testing.

The fundamental purpose of Federal security performance assessment is to ensure that requirements are properly implemented. Therefore, the primary Federal assessment organization

should ultimately report to the Chief of Defense Nuclear Security, who is responsible for requirements. This provides independence not only from the contractors, but also from the tactical-level Federal field staff whose necessary day-to-day interaction with contractor managers and staff risks loss of objectivity. This enables the Chief of Defense Nuclear Security to better ensure effective implementation of NNSA security programs. Additionally, it provides feedback on performance to the operational and tactical levels.

These Federal security assessments should include performance testing of all critical elements. The assessors should issue clear findings which are to be tracked and closed in a program-wide corrective action management system. Federal assessors should also look closely at the contractor self-assessment process; "failures to identify" by the contractor self-assessment element should automatically rise to the level of significant findings.

The final tier of the assessment model should explicitly rely upon the services of the independent security oversight function currently provided by HSS. NNSA should arrange for a regular process of comprehensive inspections. The oversight function should be encouraged to issue strong findings for matters of potential concern to the NNSA Administrator and the Secretary of Energy, and should routinely evaluate the performance of contractor self-assessments and the Federal assessment program.

This performance assessment model assumes a common requirements base that is employed at all levels and across the NNSA security program. While some allowance may be made for site-specific issues, the fundamental elements of this requirements base should be an appropriately integrated system of DOE policies, NNSA implementation directives, and field operational guidance. The requirements base should be reflected in approved documents such as site Safeguards and Security Plans. Specific performance requirements should be articulated in

detailed performance standards and criteria supported by a commonly understood and utilized performance testing process.

Closing

Over the years, there has been tension between implementation of security and conduct of operations. Whenever there have been significant incidents of security concern, there have been corresponding swings of the pendulum towards a more rigorous security program. Security program emphasis has increased after espionage cases, internal security lapses, and external events such as the September 11, 2001 attacks. However, over time, the general trend has been to accept more risk and to reduce the perceived burden and cost of the security mission. Furthermore, the trend has been to remove security from an integral mission role, adversely affecting the NNSA security program. The events at Y-12 illustrate how far the pendulum has swung in the wrong direction.

The Secretary of Energy characterized the Y-12 events as "unacceptable" and clearly stated that security is the highest organizational priority. The NNSA Administrator has been equally emphatic in numerous public statements since the incident. The evidence from Y-12 and from prior security incidents points to a culture of compromises. Moving forward, NNSA must establish and sustain an effective security program. NNSA must address the significant flaws in the current organizational structure for security and the associated assessment model. NNSA must clearly and consistently emphasize the importance of security. Ensuring that the right leadership is in the right position is absolutely critical to success. The daunting prospect—and the one that will require the consistent emphasis of current and future Secretaries of Energy and future Administrators of the NNSA—will be to instill a culture that embraces security as a

fundamental and essential element of the NNSA mission. If NNSA fails in this, then senior leaders will again find themselves answering to the American people for the failures of security. Sooner or later, the perpetrator will not be peacefully-minded.

Mr. MURPHY. Thank you. I appreciate that.

Mr. Poneman?

TESTIMONY OF DANIEL B. PONEMAN

Mr. PONEMAN. Chairman Murphy, Ranking Member DeGette, and members of the subcommittee, thank you for the invitation to appear before you today to provide the subcommittee details on the actions the Department has taken or will take to strengthen the security of the Nuclear Weapons Complex in the wake of the July, 2012, Y–12 incident. We appreciate the interest and engagement of this committee and recognize the important oversight role that you fulfill. The Secretary and I recognize the severity of the problem that led us to this point, and we have acted swiftly to identify and address the issues it revealed.

Since the Y–12 incursion, several major actions have taken place to improve security immediately and for the long term. Let me tell you about a few of them.

We restructured the contracts at Y–12 to integrate security into the line of command at the M&O contractor. The protective force contractor was terminated, and a new M&O contractor has been selected to manage the Y–12 site, providing an opportunity for new leadership and to improve the Y–12 security culture. We held accountable both the senior federal and contractor management personnel at headquarters and the site, removing them from their positions. The Department's Chief of Health, Safety, and Security conducted an independent security inspection of Y–12 security operations, which include rigorous force-on-force performance testing, as well as no notice and short notice limited scope performance testing activities as directed by the Secretary. HSS will be conducting a follow-up review in April to examine the status of the implementation of corrective actions. The Secretary also directed HSS to conduct immediate extent of condition assessments of all sites in Category I nuclear materials across the DOE complex, to identify any immediate security issues and to follow up with a full security inspection, including force-on-force exercises to assure effective security measures are being implemented at those sites.

NNSA conducted an immediate after-action report to identify causes, issues to be addressed and recommended action, and you just heard very eloquently summarized the findings of those reports.

In order to address these institutional problems that have been revealed, we are continuing to embrace and implement the findings of General Finan's report, which you just heard her describe.

Because we believe that we need fresh perspectives from disinterested parties to consider broader and long-term responses to this incident, Secretary Chu requested three independent experts in this area to conduct a strategic review of the entire DOE security architecture, with a particular emphasis on Y–12, and I see that you are joined by two of the three of these eminent experts here today. Each of them provided thoughtful advice on the DOE's nuclear security structure, specifically, all Category I nuclear facilities. We are now reviewing and discussing their advice on how to improve security at Y–12, and across the nuclear enterprise.

The series of personnel and management changes I have described today were made to provide effective security at the Y–12 site, and across the DOE complex. We are also working to carry out the structural and cultural changes required to secure all Category I nuclear materials at this and all other DOE and NNSA facilities, and in this respect, I welcome the comments of—in your opening remarks from members of this subcommittee about the need to introduce cultural changes so that we are not back in the same situation again. That is absolutely critical, and I think as we get into the discussion, what you hear in terms of what we are implementing from General Finan's report will put us in the right direction in that respect.

Our management principles hold that our mission is vital and urgent. Nowhere is that more true than here. The security of our Nation's nuclear material and technology is a core responsibility of the Department, in support of the President and in defense of the Nation. The incident at Y–12 was unacceptable and served as an important wakeup call for our entire complex. The Department is taking aggressive actions to ensure the reliability of our nuclear security programs across the entire DOE enterprise and will continue to do so.

In that effort, the Department looks forward to working with this subcommittee to ensure the security of the Nation's nuclear materials. I would be pleased, of course, to answer any questions from members of this subcommittee, and request the balance of my statement be submitted for the record.

Thank you, Mr. Chairman.

[The prepared statement of Mr. Poneman follows:]

Statement of
Hon. Daniel B. Poneman
Deputy Secretary
U.S. Department of Energy

Before the
Subcommittee on Oversight and Investigations
Energy and Commerce Committee
U.S. House of Representatives

March 13, 2013

Chairman Murphy, Ranking Member DeGette, and members of the Subcommittee, thank you for the invitation to appear before you today to provide the subcommittee details on the actions the Department has taken or will take to strengthen management, oversight, and security of the nuclear weapons complex in the wake of the July 2012 Y-12 incident. We appreciate the interest and engagement of this Committee and recognize the important oversight role that you fulfill. We also share the Committee's commitment to assure that all of our offices and operations are delivering on our mission safely and securely— from Washington, DC, to California, from every naval reactor to every warhead, from production to clean-up, from deterrence to nonproliferation.

Introduction

Since its creation in 1999, the National Nuclear Security Administration (NNSA) has served as a separately-organized entity within the U.S. Department of Energy, entrusted with the execution of our national nuclear security missions. Living up to the challenging demands of executing our mission safely, securely, and in a fiscally responsible manner requires daily management through strong, effective, and efficient relationships with our Management and Operating (M&O) contractors.

The protection of all Department of Energy (DOE) people and assets — our federal and contractor employees, technology, and physical assets, including both nuclear and non-nuclear facilities and other resources — is of integral importance to our mission. The Secretary and I know that, and understand our responsibilities to that mission, in its entirety. Indeed, we have reflected our commitment through our Management Principles, which provide that:

- We will treat our people as our greatest asset;
- We will pursue our mission in a manner that is safe, secure, legally and ethically sound, and fiscally responsible; and
- We will succeed only through teamwork and continuous improvement.

The Secretary has expressed a consistent, unwavering commitment to maintain safe and secure work environments for all Federal and contractor employees. In that spirit, we are determined to assure that the Department's and contractors' operations do not adversely affect the health, safety, or security of workers, the surrounding communities, or the Nation.

DOE's mission includes diverse operations, involving a variety of nuclear materials and processes. We recognize our unique obligations as a self-regulated agency to establish and meet exacting standards for nuclear safety and security, to maintain robust nuclear safety performance, and to provide rigorous and trustworthy oversight and enforcement of those nuclear safety and security standards. We must also maintain a safety and security culture that values and supports those standards, and assures that individuals can freely step forward to voice their concerns related to our safe execution of our mission. Indeed, we encourage them to do so. Only through these actions can we provide adequate protection of our workers, the public, and the environment, while sustaining the public trust and confidence crucial to our ability to fulfill the mission.

To achieve our mission, DOE must strive to excel simultaneously as a self-regulator, as an owner, and as an operator of the facilities in our national security complex. Each of these roles is vital and must be executed with integrity. The July 2012 incident at Y-12, as the Secretary and I have repeatedly emphasized, was unacceptable, and we have taken and will continue to take steps not only to identify and correct issues at that site, but across the DOE complex. I will address the Department's response to the incident in more detail later in this testimony.

Roles and Responsibilities for Nuclear Security within DOE

The Secretary and I bear ultimate responsibility for nuclear safety and security at DOE facilities. Under our direction, line managers have the authority and the responsibility for establishing, achieving, and maintaining stringent performance expectations and requirements among all Federal and contractor employees, at DOE labs and other facilities.

The Department's Office of Health, Safety and Security (HSS), in consultation with line management, is responsible for the development of DOE nuclear safety and security policy, Federal Rules, Orders, and the associated standards and guidance, as well as for reviewing safety and security issues complex-wide. HSS also conducts independent oversight and regulatory enforcement that is independent from line management. HSS oversight has expanded the scope and variety of performance testing methods utilized to assess the readiness of DOE and NNSA site protection systems against a defined spectrum of threats and adversary capabilities Performance testing methodologies include no-notice and limited notice inspections to obtain a more realistic assessment of site response capabilities and readiness performance.

The Department's approach to nuclear safety and security is founded on a demanding set of standards that capture knowledge and experience in designing, constructing, operating,

deactivating, decommissioning, and overseeing nuclear facilities and operations. DOE applies validated national and international standards to the maximum extent possible, because these standards reflect broad input from a large and diverse group of experts. As our management principles state: "We will apply validated standards and rigorous peer review."

Our management principles also require that we "manage risk in fulfilling our mission." This is essential to a robust safety and security culture, as demonstrated by the 2010 Deepwater Horizon oil spill, which vividly demonstrated the inadequacy of a mere "check-the-box" mentality by regulated entities when it comes to smart decision-making in a complex and hazardous operational environment. Since DOE expects scrupulous compliance with its requirements, managers and workers must recognize and embrace their personal accountability to meet safety standards, while avoiding a tendency for rote compliance with requirements. In some cases, it may be necessary to raise a hand and ask if another approach could offer a smarter way to assure safety. This questioning attitude must be encouraged.

Finally, the Secretary and I are also dedicated to strengthening contract and project management. Indeed, we cannot succeed in advancing our goals for the Department if we fall short in this effort. And, as we all know, safety and security are integral to effective contract management. Indeed, safety and security are key performance standards and elements of every contract, and extensive oversight is required to ensure stewardship as well as legal and regulatory requirements are met. When we have a safety or security problem, we must fix it, which may lead to increased costs and delays. So building safety and security into the fabric of our programs and our projects from the start and continuously monitoring adherence to safety standards is not just the right thing to do from a moral perspective, and not just the necessary thing to according to our governing laws and regulations, but it is also the smart thing to do, as stewards of our responsibilities to the Nation and its taxpayers.

Response to Y-12 Incursion Incident

On Saturday, July 28, 2012, at 4:30AM three individuals trespassed onto the Y-12 National Security Complex and defaced a building at NNSA's Y-12 National Security Complex in Oak Ridge, Tennessee.

This incursion and inadequate response to it demonstrated a deeply flawed security culture and equally flawed execution of security procedures at Y-12. In response to the incident, we acted swiftly to identify and address the problems it revealed.

Since the Y-12 incursion, several major actions have taken place to improve security:

Federal and Contractor Management Changes

New senior Federal and contractor management personnel were brought in to take charge of Site and Headquarters organizations, to transform our approach to security. Of the Federal personnel, a highly-experienced individual was appointed to serve as the new Chief of Defense

Nuclear Security and to develop overall policy; two Federal office directors experienced in security matters were appointed to implement the new policies. Of the contractor management personnel, a new M&O Site Manager and the top security official were appointed by the contractor to implement the vital security transformation.

IG Inquiry into Y-12 Security Breach

The Department and NNSA have been working diligently to implement the recommendations of the August 2012 IG report, including verifications that all critical security equipment at Y-12 has been repaired and is operational.

Protective Force Contract Terminated, New M&O Contractor Selected

WSI's protective force contract was terminated and a new M&O contactor has been selected to manage the Y-12 site, providing an opportunity for new leadership and to improve Y-12's security culture and management. The award is currently under an automatic stay while being protested at the GAO. Combining contracts and site offices will allow us to improve performance and operate as an integrated enterprise.

HSS Y-12 Security Inspection

HSS conducted an independent security inspection of Y-12 security operations, which included rigorous force-on-force performance testing as well as no-notice and short-notice limited scope performance testing activities as directed by the Secretary. The final report of inspection results was completed and briefed to senior management on September 28. The Y-12 inspection results were also briefed to Congressional staff. HSS will be conducting a follow-up review in April to examine the status of implementation of corrective actions.

Extent of Condition Reviews

At the direction of the Secretary, the Department's Chief of Health, Safety and Security also conducted extent of condition reviews at all of the DOE and NNSA Category I Special Nuclear Material (SNM) sites in collaboration with DOE and NNSA Program Offices. These reviews assessed the current security posture, specifically to determine whether the systemic issues identified at Y-12 were present at other sites, so that any necessary steps could be taken to cure any such defects. HSS completed its review in December 2012. The results were briefed to DOE leadership and Congressional staff.

Comprehensive Independent Oversight Security Inspections of all Category I Sites

The Secretary also directed HSS to conduct assessments of all Category I sites across the DOE complex, to identify any systemic security issues. These deep dives are being conducted by the HSS Independent Oversight organization, and include the HSS enhanced program of performance testing program, evaluation of force-on-force exercises, no-notice security testing,

and comprehensive security inspections at all Category I sites by October 2013. HSS has completed security inspections at Y-12, Oak Ridge National Laboratory and the Hanford Site. Results of these inspections have been briefed to DOE leadership and Congressional staff. The remaining security Inspections will include the Savannah River Site (field work completed February 21), Pantex Plant, Idaho National Laboratory, Office of Secure Transportation, the Nevada National Security Site, and Los Alamos National Laboratory.

Independent Expert Review of Y-12

Secretary Chu requested three former senior executives from Federal agencies and the private sector to conduct a strategic review of the entire DOE security architecture with a particular emphasis on Y-12. These executives included President of the Carnegie Foundation and former Nuclear Regulatory Commission Chairman Richard Meserve, former Lockheed Martin CEO Norman Augustine, and retired Air Force Major General Donald Alston. Each one provided thoughtful advice on the DOE's nuclear security structure, specifically all Category I nuclear facilities. Their words of advice and ideas are current being considered to improve security at Y-12 and across the nuclear enterprise.

Brigadier General Sandra Finan's Review

On August 14, 2012, then NNSA Administrator Tom D'Agostino commissioned a Security Task Force led by Brigadier General Sandra Finan to analyze the then-current federal NNSA security organizational structure and security oversight model, and to recommend possible improvements.

Over the course of several months, Gen Finan and the members of the Task Force conducted a thorough review of NNSA security operations at headquarters and in the field.

Organizational Improvements

Prior to the Y-12 incursion, the Headquarters NNSA security organization, the Office of Defense Nuclear Security (NA-70), served as a "Functional Manager" for the security mission, while the line authority flowed from the Secretary to other NNSA Administrators and other organizations. General Finan recommended for strategic-level policy guidance, requirements determination, and performance assessment to be under the jurisdiction of the Chief, Defense Nuclear Security (NA-70). NNSA's Office of the Associate Administrator for Infrastructure and Operations (NA-00) would provide the operational accountability for NNSA's security organization. Operational implementation and standardization of operations across the security program occurs at the NA-00 level.

The existence of a single point through which the field reports and is held accountable is the way the NNSA will assure the consistent and effective implementation of security policy. This is

a change from the approach the NNSA has taken—where each field office had greater latitude in implementing policies and requirements for its site.

Additionally, Gen. Finan made recommendations to eliminate the conflict between DOE Security Orders and NNSA NAPs. Specifically, NNSA should use DOE Security Orders. DOE has a specialized security policy function that produces its orders. Rather than attempt to duplicate this function, DOE orders would provide direction while the NAP process would provide guidance and clarify information in the orders as appropriate, but not reduce requirements.

Changing the Assessment Model

Regarding NNSA's security oversight model, Gen. Finan found that at the time of the Y-12 incursion NNSA did not have an adequate security performance assessment process or capability. The systems-based assessment model that was employed was ineffective for security. NNSA lacked a clear and consistent performance baseline for security program implementation and the assessment model was biased against criticism.

To directly address problems with the assessment model, NNSA has set about implementing a three-tiered approach to assessing security throughout the NNSA. This approach includes: 1) an initial assessment performed by the contractor at the site, 2) an assessment of the contractor's performance carried out by the Chief of Defense Nuclear Security at DOE Headquarters (NA-70), and 3) independent oversight by the Office of Health, Safety and Security. And, of course, apart from this three-tiered assessment and inspection regimen, we expect Federal site personnel to perform quality assurance activities on a routine basis as an integral part of their line management responsibilities.

The Secretary and I are pleased that the NNSA has responded to Gen Finan's recommendations seriously and is on a course to implement effective security improvements.

The series of personnel and management changes I have described today were made to provide effective security at the site and across the DOE complex. We are also working to carry out the structural and cultural changes required to secure all CAT 0/1 nuclear materials at this and all other DOE and NNSA facilities.

Conclusion

In conclusion, the security of our Nation's nuclear material and technology is a central responsibility of the Department, in support of the President and in defense of the Nation. We must remain vigilant against error and complacency and have zero tolerance for security breaches at our Nation's most sensitive nuclear facilities. The incident at Y-12 was unacceptable, and it served as an important wake-up call for our entire complex. As a result, the Department is carefully reviewing security at all of our NNSA sites – as well as all of the recommendations of the HSS security review teams, Brigadier General Finan, DOE IG, and independent reviews provided by distinguished military and private sector experts – with a

view to taking all those steps that are needed to protect this Nation's most sensitive materials and technologies. The Department is taking aggressive actions to ensure the reliability of our nuclear security programs across the entire DOE enterprise, and will continue to do so.

We accept the responsibility that we have inherited from the generations of Americans going back to the Manhattan Project to assure the safe and secure stewardship of our nuclear enterprise in order to deter aggression, defend our freedom, and support our allies.

In that effort, the Department looks forward to working with the Committee to ensure the security of the nation's nuclear materials. I would be pleased to answer any questions from members of the Subcommittee.

Mr. MURPHY. And so will the balance of your statement will be submitted for the record.

We understand, Ms. Miller, you do not have an opening statement, so we will go right into some questions. I will recognize myself for 5 minutes.

First of all, let me just say that I appreciate your candor. Nothing is better for leaders than to step forward and say mistakes have been made, taking full responsibility, and taking definitive action. I thank you for that. We are certainly hoping this never happens again, and we hope that the report and recommendations are going to be fully implemented and continue to be reviewed.

So let me start with you, General Finan. Your task force identified the serious weaknesses in the federal capability to evaluate contractor performance at the Nuclear Weapons Complex. The NNSA administrator commissioned your report. I am correct in that?

General FINAN. Yes, sir.

Mr. MURPHY. It is also correct that the recommendations are directed at the administrator, not the Secretary of Energy, am I correct?

General FINAN. That is correct. It was all NNSA-focused.

Mr. MURPHY. Thank you. I just want to make sure we are following the right chain here.

Mr. Poneman, as Deputy Secretary of Energy, you and the Secretary set high level policy direction and safety and security standards for NNSA's mission, but it is the responsibility of the NNSA to arrange a structure to accomplish these goals. That is up to the administrator, am I correct?

Mr. PONEMAN. It is up to the administrator, of course, subject to, as you just said, the leadership of the Secretary and the Deputy Secretary.

Mr. MURPHY. And something you will continue to monitor as well?

Mr. PONEMAN. Absolutely.

Mr. MURPHY. Thank you.

Ms. Miller, you are now the NNSA Acting Administrator.

Ms. MILLER. That is right.

Mr. MURPHY. Is it correct that you were Principal Deputy Administrator at NNSA as it implemented its safety and security reform efforts in 2010?

Ms. MILLER. I became the Principal Deputy Administrator in August of 2010.

Mr. MURPHY. OK. Do you agree with the findings of General Finan's report?

Ms. MILLER. I completely agree with them.

Mr. MURPHY. Thank you.

General Finan states that NNSA must clearly and consistently emphasize the importance of security. Do you agree with her statement?

Ms. MILLER. I absolutely agree with them.

Mr. MURPHY. Thank you.

Do you believe that NNSA's leadership has been inconsistent in the message it sends to the field about security emphasis?

Ms. MILLER. I believe it has been inconsistently communicated, yes. Absolutely.

Mr. MURPHY. Were you aware of the inconsistent messages on security prior to Y–12?

Ms. MILLER. I would say that I was aware that because the chief of Defense Nuclear Security, as well as the chief of Defense Nuclear Safety reported directly to the administrator and not to me. I would say I was aware of the difficulty and the inconsistencies in communicating policy and decisions for security and many other areas from the headquarters organization to the field offices.

Mr. MURPHY. Well yes, and since part of the purpose of this Committee on Oversight is to make sure that we are understanding lessons learned, but what you don't measure, you can't manage. What you don't admit, you can't act on. Were there some lessons you learned from this, some things that you should do differently in terms of the process as we move forward?

Ms. MILLER. Mr. Chairman, I would say two things. First of all, there were lessons I had been learning prior to this incident that caused us to announce a few weeks before this incident, the end of July, that we were changing the way we governed our sites. And that is to say, we took the sites from within defense programs, our large weapons program, where they had been reporting for a number of years and had them now directly report to the administrator through an associate administrator peer level, the senior management, so that we could start to drive accountability and consistency across our sites. So that was a measure that I had come to the conclusion that organization absolutely had to make to address what I said before, which was concern about inconsistencies all over the place.

With regard to post-Y–12 incident, in particular with security, I was fortunate to be able to draw upon General Finan's recommendations and work with her, as she was part of the organization at the time, and others to change the way we operate security, both at headquarters and in the field.

Mr. MURPHY. Thank you.

Last month on February 5 at NNSA, associate administrator for management and budget disputed the Inspector General's report that Y–12 oversight was ineffective because of the "eyes on, hands off" oversight approach. The officials said that the "eyes on, hands off" policy never applied to security matters and that this was a misperception by some federal officials. Ms. Miller, why is an NNSA senior official continuing to dispute the impact of the "eyes on, hands off" policy?

Ms. MILLER. I think the issue is not to dispute the impact. I think the point is that we certainly did not set out—and again, this predates me, but no one set out to say that oversight should not be conducted, that your proper role is not to be overseeing all aspects of the contractor's performance. What I would say is that, as you yourself mentioned, driving that message through a very large organization from the administrator through every individual in every layer at every site is the big challenge. It is the challenge in security, it is the challenge all over the place. It is not a new issue. As the ranking member mentioned, we need to break the pattern, and that is definitely what the organization is about right now.

Mr. MURPHY. Thank you. Hopefully you will communicate that through solidly, because of the extreme concerns about what happened.

I recognize each member for 5 minutes as we go through. Next is Ms. DeGette.

Ms. DEGETTE. Thank you, Mr. Chairman.

Secretary Poneman, I was intrigued when—first of all, let me say, I am impressed and encouraged by the commitment the agency has made to not having to come back here next year or the year after with some new crisis. I am, both in these hearings and some of our off—our side conversations, I do believe you have that commitment.

Secretary Poneman, I wanted to ask you, because you just said in your testimony that you are committed to implementing some of the aspects of the General's report to make sure that we are not back here in a year or two. I wonder if you could briefly tell us—if you could give us the highlights of what those things are?

Mr. PONEMAN. Gladly, Congresswoman DeGette.

The critical, I think, finding that General Finan's report showed was that we had a lack of clarity of line of management control and accountability. So what we have done is, under her recommendation implemented by Acting Administrator Miller and fortunately, before General Finan left us, she was the acting head of defense nuclear security, to get this started. We have now made sure that under this organization that Ms. Miller just introduced of the operations and infrastructure that the responsibility to direct security at the site flows down from the administrator through that office to the site. The other office that had been doing security policy, so-called NA–70, had been actually exercising some apparent line management authority, which was creating confusion. That function has been stripped away. Any line authority has been stripped away from NA–70.

Ms. DEGETTE. So you think that is the key, having a clear chain of—that is the number one? What else?

Mr. PONEMAN. Number two is the staff function that that new organization—that NA–70 must perform, they need to promulgate the policies and perform independent evaluations so it is not just the site checking itself.

Ms. DEGETTE. OK, independent evaluations. Those are the two key things.

Mr. PONEMAN. Yes, oversight and a line management.

Ms. DEGETTE. Now, another issue—I don't have—we might do another round, but—so I want to just go into this other issue that I care a lot about, which complaints that the committee has heard about overly burdensome oversight stifling the work being done at NNSA labs and sites. And what we think—I was talking to the chairman about this—is that federal officials need to conduct strict oversight of the contractors, or serious security problems can fall through the cracks.

So what I wanted to ask you, General Finan, in your review, did you find that the problems you saw within NNSA were caused by overly burdensome congressional oversight?

General FINAN. The issues that I found were not caused at all by oversight. It was actually caused by lack of oversight, and I mean oversight at every level.

Ms. DEGETTE. Right, right. So what was the——

General FINAN. It was impacting everything.

Ms. DEGETTE. We need to have clear oversight from the top down, and as Mr. Poneman says, independent oversight, right?

General FINAN. The burden was actually—when you—we created a system that required a whole bunch of paperwork, and the paperwork is burdensome, but what we lost in security was the ability to see security performance. It was paperwork.

Ms. DEGETTE. Yes, there was a bunch of paperwork, but it was irrelevant to the core task, right?

General FINAN. Correct.

Ms. DEGETTE. Mr. Poneman, do you want to comment on that?

Mr. PONEMAN. I thought it was a very apt finding, and the misinterpretation of that 2010 reform is exactly on this point. We were trying to strip away the excessive paperwork and get to the performance testing.

Ms. DEGETTE. Right, but did any of the auditor's assessments conducted in the wake of the Y–12 incident find that it was caused by too much congressional oversight of the Y–12 contractors?

Mr. PONEMAN. No, ma'am.

Ms. DEGETTE. OK. The reason I bring this up is because some people try to say oh, we have too much oversight. It seems to me when we have these problems over and over again, the problem is not too much oversight. The problem is too little effective oversight and accountability. Ms. Miller, you are nodding your head. Would you agree with that?

Ms. MILLER. Yes, I would definitely agree. It is about effectiveness.

Ms. DEGETTE. Now, let's see.

General Finan, can you tell us about the findings of the task force with respect to improved oversight of NNSA security contractors? You touched on it just very briefly.

General FINAN. Right. The recommendation we are making is that we create an NNSA oversight function, because right now, in the system as I looked at it a couple of months ago, NNSA did not have any oversight capability. They depended on onsite federal personnel to analyze contractor performance. But again, they were applying the "eyes on, hands off" concept and so that was varied from site to site. And what happened is that you lacked—there was no sense of criticism in this assessment, right?

Ms. DEGETTE. Right.

General FINAN. You had onsite people who were your really only federal ability to look at contractor performance. Well, those folks onsite grew up there, they lived there, you know, they spent their whole time. They identified with the mission and they were really not a very good source of independent oversight as to contractor performance.

Ms. DEGETTE. Thank you.

Mr. Poneman and Ms. Miller, do you agree with that?

Mr. PONEMAN. Absolutely——

Ms. MILLER. Yes.

Mr. PONEMAN [continuing]. And the reforms we described I think reflect that finding.

Ms. DEGETTE. Thank you.

Ms. Miller, do you agree with that?

Ms. MILLER. I do.

Ms. DEGETTE. Thank you.

Mr. MURPHY. Thank you. Gentlelady yields back.

I now recognize the gentleman from Ohio, Mr. Johnson, for 5 minutes.

Mr. JOHNSON. Thank you, Mr. Chairman.

Mr. Poneman, in her testimony, General Finan states that NNSA must clearly and consistently emphasize the importance of security. Unfortunately, here is the consistent message that the DOE, NNSA organizations, and contractors were hearing. In March of 2010, Secretary Chu stated his vision that he wanted DOE to be viewed as a valued partner and asset to contractors. He went on to suggest that safety could be ensured with a skeleton crew of health and safety experts. Also in March of 2010, Mr. Poneman, you wrote in the Department's safety and security reform plan that success will be measured through near-term relief from specific low-value burdensome requirements, as well as longer term streamlining of requirements that will lead to measurable productivity improvements. I note that safety and security did not factor into this definition of success. Would you agree that statements like these send mixed signals about the Department's commitment to safety?

Mr. PONEMAN. Congressman, the portion of the document read from my document, the genesis of that was to set out a set of safety and security objectives, so in fact, that particular sentence is out of documents that are precisely intended to maximize safety and security. What is unfortunate, what has happened is the misinterpretation of that. What we were trying to do, sir, is to get rid of the checkbox mentality, just looking at paperwork and creating paperwork, get back to performance testing, so we could be better, safer, and more secure. That is absolutely our objective.

Mr. JOHNSON. What are you doing today to ensure consistent and clear emphasis on safety importance from the headquarters on down?

Mr. PONEMAN. Number one, we are, on both safety and security, assimilating all of the learnings from reports such as General Finan's. Number two, because we have found safety culture issues as well as security culture issues, we have regular meetings where we assemble the top leadership in the Department to check on a continuing basis that this is being messaged consistently throughout the complex. One of the major challenges, Congressman, that we have found is—as you heard with this talk about "eyes on, hands off"—is the misinterpretation, like a kid's game of Telephone, is a terrible problem. So it is not enough to promulgate a good policy. You have got to continually stay on it, message it, and work with your leadership and work with the people in the field.

Mr. JOHNSON. OK, thank you.

Ms. Miller, a week or so before the Y–12 incident in July of 2012, Mr. Don Cook, NNSA Deputy Administrator for Defense Programs, made the following remarks, and I quote, "With regard to the relationship that we have and where we are between NNSA and its

labs and plants—I didn't say my labs and plants, but you can tell I feel that way—getting to the point where we have oversight on these, which is eyes on, hands off oversight, has been my aspiration for several years and it remains so. It was my aspiration when I worked on the lab side for many years. General Finan completed that ensuring that the right leadership is in the right position is absolutely critical to success." What are you going to do to make that happen, ensure that leadership is sending the right message about the importance of safety and security?

Ms. MILLER. Mr. Johnson, sending the right message, in my view and after many years of looking at the NNSA mostly from outside of it, is a challenge that is not achieved just by making sure that people at the top level know what the message means. But it is difficult to make sure that every single person in the 10,000 people at a given lab or 30,000 throughout our complex understand what we are talking about. If we—what we are doing at NNSA is working to be able to communicate and train and talk to people at every single level to make sure it is not going to be misunderstood. We recently changed all of our M&O contracts. The performance measures in those contracts are all now connected to safety and security so that it is not possible to believe that you have performed according to the terms of a contract in an area like nuclear weapons if you have not also met the performance plans for safety and security. It just isn't going to happen.

So this is a step-by-step throughout the organization. It is not just at the top level.

Mr. JOHNSON. OK, good.

One final question, General Finan. First of all, as a 26½ year veteran of the Air Force myself, thank you for your service and what you have done here.

A troubling finding in your report is that potentially critical management information is not being reported clearly to the appropriate decision makers. Would you elaborate on what you mean by this?

General FINAN. Yes, sir. As we interviewed people and took a look at what was happening, we found out at the lower levels, there were people who knew what issues existed out there and knew the significance of those issues. But as they attempted to rise those issues up to senior levels, they were being suppressed. Management at mid levels would suppress it, and so in many cases, critical decision information was not making its way to the top of the organization.

Mr. JOHNSON. OK, thank you for that, and with that, Mr. Chairman, I yield back. Thank you.

Mr. MURPHY. OK, gentleman's time is expired, and I will now recognize Mr. Tonko for 5 minutes.

Mr. TONKO. Thank you, Mr. Chair.

General Finan, you state in your testimony that the findings of this task force were very similar to those numerous prior reports by other review teams, so my question is, what happened to the recommendations of the prior review teams? Were they ever implemented? Was the implementation insufficient, or is there a larger problem that still needs to be identified?

General FINAN. There is a cultural issue. Those findings, as you look at them, you go back to see what people did, you will find that there are some actions that were put in place, but there was a check the box mentality that said we want to get rid of the findings as fast as we can. So they do whatever they could to say yes, I have responded to this finding and it is gone. And so the things that they changed didn't stick. It was just a matter of taking action, checking the box, closing the finding, and going on to the next thing. And so what needs to happen is all those things need to be taken in aggregate, we need to create a roadmap, and then we need to change the culture so that we continuously evaluate those things and go back and make sure that we don't, year after year, make the same mistake and that we are not interested in checking the box off, we are interested in changing the way we do business so we do it the right way.

Mr. TONKO. Thank you. There seems to be a theme that runs through a number of the task force's observations that cost control was a bigger concern for many of the people managing the program, the security program, than performance of the security mission. This implies there is a real or perceived lack of resources to support the security mission fully. Which is it, real or perceived?

General FINAN. It is a combination of both. What happened was that management had overwhelmingly started to figure out—they wanted to reduce the cost of security, and so in doing that, what they did is they lost sight of the requirements of security, and because the two were mixed together, the people who determined requirements and the budget were the same people. What happened was that they were no longer looking at the actual requirements for security. They lost sight of what was required in order to adequately secure these materials and these sites, and moreover, they lost visibility on the important aspect of protecting our operational capability and our people. And those items actually got no visibility at all and were completely ignored. They thought that if they could do the big war, if they could fight the terrorists, they could do all the lesser includeds, therefore, they never needed to look at lesser includeds. Well, lesser included happened to be a protest event, and Y–12 proved that lesser includeds do not—you cannot do lesser includeds just because you can fight the larger issues. So it was a combination of wanting to reduce the budget, which is a good thing. We ought to always be efficient, but when you lose sight of the requirements, what happened is senior leaders at NNSA did not get to make the decision. Do I want to fund that requirement or do I want to take the risk? The risk was being assumed at lower levels by default rather than being made at the senior decision maker level at NNSA.

Mr. TONKO. Deputy Secretary Poneman—and I thank you for that answer—but Deputy Secretary, how much of DOE's budget is spent on contractors, your area of the budget?

Mr. PONEMAN. The vast majority. I think it is well over 80 percent, and we can get you a precise number. I think it is on the order of 85 percent.

Mr. TONKO. With that amount, the agency then, is it fair to say, is relying on private contractors to implement many key security and safety goals?

Mr. PONEMAN. Yes, Congressman, going back to the origins of the Department, back to shortly after World War II, Atomic Energy Commission, this whole model of the so-called management and operating contractor, the M&O contractor model puts most of the programmatic and security burdens in the hands of contractors who were exercising that authority under federal oversight.

Mr. TONKO. So do the contractors then have a conflicting bid of incentives here when carrying out their duties?

Mr. PONEMAN. There is a risk, Congressman, and in that respect, again, one of the many fine findings of General Finan's report, I think, shows the way we need to address that is the contractor must own and take responsibility for security, and in the first instance, must evaluate that under their own self-analysis, but that then needs to have a double check, first from the headquarters so there is not the onsite cozy relationship, so there is some difference and the federal oversight is effective, and secondly, from an independent organization, the HSS organization, to effectively ensure you have a disinterested third party look to make sure that that security is being well executed and there are not conflicts of interest, and to hold the contractor accountable if they do not self-disclose problems in security that they, in fact, find in their own forces.

Mr. TONKO. General Finan, is it possible that contractor concerns over cutting costs could have been one of the causes of the Y–12 incident at Oak Ridge?

General FINAN. It could have been, and it may have been that they had cut back some of their maintenance personnel in order to cut costs, and therefore had misprioritized actions, so it could be a contributing factor.

Mr. TONKO. Thank you. With that, I yield back.

Mr. MURPHY. Gentleman's—thank you very much.

The chair recognizes the chairman emeritus of the committee from Texas, Mr. Barton, for 5 minutes.

Mr. BARTON. Thank you, and I appreciate the courtesy of letting me ask questions out of order, since I wasn't here at the beginning. I appreciate that of my junior members.

I want to refresh the subcommittee's memory a little bit. We have had repeated security incidences at the weapons complexes in the national laboratories over the last 20 years. We have had tapes lost, we have had materials lost. This latest incident, which has been sanitized to call the Y–12 incident, three nuns, I think, one fairly elderly, penetrated to the deepest security of our weapons complex. A nun, oK, nuns. They showed up at one of our hearings and they were in the audience, and these were not ninja warrior, flat belly, skulking people. These were just ordinary folks who wandered in, so to speak. So we have, once again, another task force that is going to try to rectify the problems.

Now, I want to get the players straight. General Finan, you are not in the normal chain of command at the Department of Energy, is that correct?

General FINAN. I am no longer assigned to the Department of Energy. I am back in the Air Force. I was always in the Air Force, but——

Mr. BARTON. This report that you have helped to prepare was done at the request of DOE, at the request of the then administrator, but you were kind of an outside, fresh look person, is that correct?

General FINAN. Well, I guess I would call myself an inside outsider. By that time, I had been assigned to NNSA for 18 months, but I was always an Air Force asset. My reporting chain runs through the Air Force. I was always an Air Force member, but I was assigned to NNSA for 2 years.

Mr. BARTON. OK, now the report that you testified on has been presented to the Department of Energy, is that correct?

General FINAN. Yes, sir.

Mr. BARTON. Now I want to go to Deputy Secretary Poneman. It used to be the Deputy Secretary is the number two person at DOE. Is that still the case?

Mr. PONEMAN. Yes, sir.

Mr. BARTON. Are you the chief operational officer at DOE?

Mr. PONEMAN. Yes, sir.

Mr. BARTON. OK. So you have read the report——

Mr. PONEMAN. Yes, sir.

Mr. BARTON [continuing]. That has been prepared? I have read a summary of it. It is fairly damning, but it is pretty clear cut in its recommendations. So the bottom line question is what are you going to do about it? Are you going to accept the recommendations and act on them, or are we going to pontificate and fiddle faddle around and not do anything?

Mr. PONEMAN. Yes, sir, it is a fine report. It is excellent. It is insightful. We embrace it and not only have we already accepted and put into practice the recommendations, but while we still had the benefit of General Finan's service in the Department, we made her Acting Chief of Defense Nuclear Security to oversee the beginnings of the implementations.

Mr. BARTON. So she gets to implement the recommendations?

Mr. PONEMAN. She had that started, and as she just indicated, been reassigned and we are carrying forward from that.

Mr. BARTON. One of the recommendations is that you eliminate this multiple diverse authority. Is that going to be done, centralizing the one line of authority? That is one of the primary——

Mr. PONEMAN. That, sir, already has been done and the further clarification of the role of the other security organizations is also underway. We are, as was indicated, also taking into account more widely the recommendations from what we call the Three Wise Experts about—from whom you will hear directly, but the parts that you have heard from General Finan, we are already putting into effect.

Mr. BARTON. OK. Now this concept of "eyes on, hands off" oversight, there seems to be some misunderstanding about that. I don't see how that would work anyway.

Mr. PONEMAN. I don't either, and I think it is a terrible thing that anyone ever thought that that made sense or was the policy of the Department. It is absolutely the wrong way to think about it.

Mr. BARTON. So we can assume, since you are the number two person, that whatever that concept was, it is no longer in use? It is gone?

Mr. PONEMAN. Yes, we have tried and we will continue, because you can't repeat these messages often enough, to be very, very clear that the federal oversight is critical and it needs to be active and performance-based, and it cannot be "eyes on, hands off." That would never work.

Mr. BARTON. OK, now my final question, can we be—can you assure the committee that the actual security of the weapons complex is a first-degree, primary function and it is not subject to cost issues? I mean, we want these facilities and materials and the people that are operating within those facilities to be secure, period, and not secondary to the cost of maintaining the security.

Mr. PONEMAN. Let me be very clear, Congressman. There is nothing more important than the safety and the security of the complex. That is our top priority. We will always, as you would expect, make sure that we are good stewards of the taxpayer resources and not waste money. I don't think that is the implication of your question, but we will always make sure that we never compromise security for any other derivative objective, and the security of that material is paramount.

Mr. BARTON. Thank you, and thank you, Mr. Chairman and the other members. I yield back.

I would love to have a hearing within the next year or two where we can pat these people on the back and say you have actually done what you said. Things are working. There are improvements. Now, I am a skeptic. I doubt we will have that hearing, but I certainly hope that we can and I especially want to commend Congresswoman DeGette. She has been fighting these fights almost as long as I have, and with the same degree of fervor and intensity, and I am sure that with Dr. Murphy's added vigilance, we might actually get something done. Thank you.

Mr. MURPHY. Thank you. We all share sentiments. Gentleman yields back.

Now recognize the gentleman from New Mexico, Mr. Luján, for 5 minutes.

Mr. LUJÁN. Thank you very much, Mr. Chairman.

Mr. Poneman and Ms. Miller, before I ask some questions on Y–12, I want to speak about something that is very important in New Mexico. With the concerns in Washington State where tanks at Hanford are leaking radioactive and hazardous waste, I understand the Department is considering sending millions of gallons of highly radioactive waste to New Mexico to be stored at the Waste Isolation Pilot Plant, or WIPP. I would like to get your commitment here today that you will work closely with the New Mexico delegation, state and local officials, and concerned citizens, as you explore whether such a transfer will take place and under what conditions?

Mr. PONEMAN. Congressman, I can assure you, A, that we always take all critical health, safety, environmental issues into account, certainly with respect to the 54 million gallons and their disposition at Hanford, and we will gladly continue to work very closely with this committee and with other members of the Congress to make sure what we do is in full consultation with you.

Mr. LUJÁN. So Mr. Poneman, that is a commitment to work with the New Mexico delegation on this issue?

Mr. PONEMAN. We will work with this committee and with all members of Congress, and any affected state——

Mr. LUJÁN. I will interpret that as a yes. I appreciate that, sir.

Has there been discussions that have begun with the State of New Mexico on this issue?

Mr. PONEMAN. I will defer to Ms. Miller.

Ms. MILLER. The acting Assistant Secretary for Environmental Management, Dave Huizenga, has ongoing discussions with representatives from the State of New Mexico. I recently met with a number of representatives from the State of New Mexico, local representatives as well as the governor. We did not discuss this issue because this is a pretty new development, as you know, but we are in good, close contact with the delegation, both locally and certainly as Deputy Secretary Poneman said, very willing to work and look forward to working with you and the other members of the congressional delegation.

Mr. LUJÁN. I appreciate that, Ms. Miller. I am one of the representatives as well that represents New Mexico, and so I would appreciate that very much. I appreciate that.

And finally, I hope that this will not happen at the expense of cleaning up existing sites in New Mexico. I don't want to see a slowing down or a decrease in funding in environmental management funding. If anything, it should be increased to allow more rapid cleanup, especially in Los Alamos. And you know, with the true waste issue in New Mexico, it is ready to be cleaned up and ready to go, and I hope that we can work with you and get a commitment to see what we can do to plus up those accounts. I know sequestration is hitting us, but it is something that is very important to us.

Mr. PONEMAN. Congressman, sequestration is a huge challenge for all of us. We have legal, contractual, and moral obligations to the state. We take them very, very seriously. I have been there several times myself. We will continue to take that seriously.

Mr. LUJÁN. I appreciate your commitment, Mr. Poneman.

Mr. Poneman, isn't your head of Health, Safety, and Security, or HSS, the person you and the Secretary rely on for developing and coordinating security policy and providing independent oversight and enforcement?

Mr. PONEMAN. That is true.

Mr. LUJÁN. Wasn't this a colossal failure as a part of HSS in failing to identify and correct the specific security weaknesses that were obviously present at Y–12?

Mr. PONEMAN. Sir, there were a number of failures. There was a January, 2009, report from HSS which, in fact, identified some of the deficiencies which you have heard later described which, in fact, facilitated this terrible episode on July 28. There should have been, as HSS has acknowledged, more rigorous, vigorous, and repeated follow-up from those findings, and they have—in the consequences in terms of lessons learned from this episode, redoubled their commitment under the direction of the Secretary to make sure that they follow up on all such findings in future. So when they do identify a problem, they stick with it until it is resolved.

Mr. LUJÁN. With that being said, Mr. Poneman, aren't those on the second panel, including reviewers like General Finan, who are identifying systemic security problems and recommending improvements, doing the job that HSS was supposed to have done?

Mr. PONEMAN. Well, it is always good after an episode like this to get fresh eyes, and General Finan, because she had this unique perspective of being in the system but somewhat apart from these specific events, had a unique and invaluable perspective. In fact, her own report recommends that in this three-layer oversight review, that the HSS is, in fact, that third layer of disinterested third party oversight. We will hopefully continue to benefit from outside expertise of this character, but also make sure we maintain some independence within the Department to ensure you don't have conflict of interest in overseeing security.

Mr. LUJÁN. I appreciate that.

Mr. Poneman, in your earlier comments made before similar hearings, you stated that no federal employees have been terminated as a result of the Y–12 breach, that such terminations are subject to due process. Since there were contract employees that were terminated for cause, the response seems to suggest that contract employees don't have the same due process protection under the law. Is there any truth to that?

Mr. PONEMAN. This is—I am glad you asked this question, Congressman. Let me clarify this. There was accountability on both the federal and the contractor's side. On the federal side—and we had to act swiftly and effectively to remove anybody who had an involvement in this episode from the chain of command. On the federal side, the top three nuclear security officials in headquarters were removed from those responsibilities. In addition, three members at the site from the federal team were either reassigned or removed from their positions. And then on the contractor's side, we held accountable by making clear to the contractor that they had lost our confidence. The three senior—three of the senior people on the protective force subcontract and three of the senior people on the M&O contractor, we then folded the subcontract for security under the M&O contract, made it clear we lost confidence in the contractor, and that contractor was terminated full stop.

Now there are additional actions that can be taken with respect to individuals that are disciplinary in nature. Our first responsibility, as the chairman and ranking member have emphasized, is to protect the material, so the first thing we did is get anybody who had anything to do with this out of the way of possibly protecting material that we now needed to make sure we had new people and new processes to effectuate. Other disciplinary processes have been underway. Some are still continuing, and those are the processes, sir, that I was referring to where the due process protections apply to these individuals who, like any American, are entitled to due process when it comes to termination.

Mr. LUJÁN. Thank you. Mr. Chairman, as I yield back, I know time is expired, but I appreciate the concerns and the statements associated with new culture and leadership and changes, and what that means coming forward as we look at the future. Thank you, Mr. Chairman.

Mr. MURPHY. Thank you, Mr. Luján. I let that go on because it was a particularly important answer, too. We thank you for that answer.

Now recognize the gentleman from Mississippi, Mr. Harper, for 5 minutes.

Mr. HARPER. Thank you, Mr. Chairman, and welcome to each of you on what is a very important topic, not only to you, but to everyone in Congress. We appreciate the look you are taking at this, and of course, how do you convey that security is everybody's concern, and always in that situation where you are looking, it seems that it was somebody else's responsibility, so you have to create that culture that everyone is responsible, regardless of their position, and do you feel like you are moving things in that direction with NNSA?

Mr. PONEMAN. Yes, sir, and your comment, I think, ties in well with when the chairman said at the beginning, if you don't measure it, you don't manage it. What we have done since the Y–12 episode is to make sure that in the performance evaluation plans for all contracts that safety and security is made a constituent part of every programmatic deliverable. So you are not actually performing the job if you do it, but you don't do it safely or you don't do it securely. So that is how we measure and hold people accountable, and so not only are we trying to do this through all the cultural teaching that we are telling you about, but we are trying to build into the structure of the contracts. That is how we hope to avoid keep coming back, as Ms. DeGette has suggested, by really building it into our system.

Mr. HARPER. And I guess one of the issues would be how do you make these security changes or improvements, how do you sustain those? You know, I will go back, DOE did a major—a comprehensive study back in 2008, and it looked like that was great. If those things had perhaps really been sustained, maybe we wouldn't have had the Y–12 incident. So I guess what confidence should we have and do you have that these changes, as a result of this very extensive 90-day evaluation and study, will be sustained?

Mr. PONEMAN. Congressman, as General Finan's report makes clear, even if we have put all the structures in place to be successful in a way that we have not succeeded so far, absent leadership, it is not going to succeed. So the first way to sustain it, sir, is by sustained leadership attention, and I can commit to you that that is what we are providing.

The second thing I would say is, it is not enough simply to promulgate this and announce it. We have to continue to work with people in the complex at the sites and have a continuous flow of information back and forth.

And the third thing is, people have to feel comfortable throughout the site. If they actually have concerns, they have to feel free to step forward without any fear of retribution.

Mr. HARPER. Thank you.

Do either of the other witnesses have anything that you care to add? General, anything that you see of how this study—how you believe it would be sustained in the future? It looks great today, and we believe we have done that, but do you see anything else,

other than what Mr. Poneman has added, that you believe would show that we could sustain it?

General FINAN. The key is the leadership, just the Deputy Secretary stated, and a culture. Everyone in the organization has to understand that each and every one of them are a part of security, and that security is a part of the NNSA mission. It is not a support item, it is essential to the mission. So it is culture and leadership.

Mr. HARPER. Mr. Poneman, the safety and security reform plan, if I could read this, stated that the Department's contractors maintain an assurance system that provides reliable measurement of the effectiveness of their safety management systems and facilitates timely corrective actions to systems or performance weaknesses. And the same direction was given for security systems. The task force found that NNSA relied overwhelmingly upon contractor-provided data rather than effectively reviewing performance itself. Given the broken equipment, security cameras, excessive false alarms at Y–12, clearly the contractor did not correct performance weaknesses in a timely fashion. And I know you have gone over this, but I want to make sure, you believe that relying on contractors to provide measurements of their effectiveness is still a sound approach?

Mr. PONEMAN. I think the system must start because they have the line management responsibility with contractor reporting and self correcting, but it then needs exactly the oversight that General Finan recommended, number one, from the nuclear security operation inside NNSA, which is not at the site and therefore it is not prone to the coziness that has been a source of some concern, and then secondly, with a third party independent oversight from the HSS organization.

Mr. HARPER. Each of you, do you believe that today would such a breach at Y–12 that occurred in July of 2012, do you believe that would occur today?

Mr. PONEMAN. No, sir, I do not, and one thing that we did immediately, the Secretary directed an extent of condition review to be done very quickly to ensure that no similar problems existed at any of the other sites that have Category I nuclear material in the complex.

Mr. HARPER. I yield back.

Mr. MURPHY. The gentleman yields back.

The gentleman from Texas is recognized for 5 minutes.

Mr. GREEN. Thank you, Mr. Chairman.

Mr. MURPHY. The gentleman Mr. Green from Texas is recognized.

Mr. GREEN. Different member from Texas.

I know there was some contract restructuring in 2007, and I guess what got my attention on Y–12 and also the Pantex site, since that is in north Texas, was that contract restructuring ever completed to have one contractor for both sites?

Mr. PONEMAN. Yes, sir, we have finished the contract consolidation. There is another piece that is optional with respect to folding the tridium operations at Savannah River, but that part has not——

Mr. GREEN. I know on a regular occasion, Pantex—there are protesters up there, but it is a long way to get there from most urban

areas in north Texas, but there has never been any similar incidents like at Y–12 at Pantex, has it?

Mr. PONEMAN. Not that I am aware of, sir, and in fact, we were impressed when we looked after the Y–12 incident at, frankly, the contrast and we brought some expertise from Pantex to Y–12 to help instill some best practices. For example, the practice of repairing cameras very quickly, that was already institutionalized at Pantex, and now I am happy to say, all the cameras are fixed and our average time to repair cameras now at Y–12 is 6.5 hours. So there were some best practices that we ported over from Pantex.

Mr. GREEN. OK. I worry about impacts on NNSA due to the sequester. Deputy Secretary Poneman, can you talk about the impacts that sequestration may have on federal and contractor personnel at NNSA?

Mr. PONEMAN. Yes, I will let Acting Administrator Miller offer more detail, but top line is it is a significant effect involving personnel and operations as well, but I can assure you, Congressman, is that the directive from the President is to do everything that we can and must do to protect our core functions. But I will ask Ms. Miller if she has got elaboration.

Ms. MILLER. I would just add to that. It starts with of course, we will protect the material, of course, we will do things safely. As long as we are allowed to operate, that is exactly how we will run things. Having said that, I think people have a tendency to look at sequestration in terms of numbers of people who might be furloughed or dollar numbers that might be missing. It is—what is a deeper concern at this point is the ongoing disruption to activities that will take projects and programs and make them difficult, if not impossible, to actually execute anywhere near to the plan and to the price and the need that has already been described. It is that ongoing uncertainty disruption, and then lack of ability to plan.

Mr. GREEN. And I know that is impacting your agency, but it is also impacting——

Ms. MILLER. Everybody.

Mr. GREEN [continuing]. Everybody.

Have you already notified employees or contractors on they could face personnel actions?

Ms. MILLER. Contractors, their own organizations are responsible for talking directly to their employees, because they operate in general off of the money they are getting for us. We have, of course, worked with them to try to plan and program dollars so that they have some sense of what it is going to look like going forward month by month, and they are making plans and doing notifications accordingly, and I know our contractors have done that.

As far as the federal workers are concerned, I sent a note out to our federal workers 2 weeks ago, almost 2 weeks ago, to let them know that we will do everything we can, but I cannot guarantee that it is not going to affect them either.

Mr. PONEMAN. And I would only add, Congressman, that I have notified all the affected governors, and we will also work with the states in the same vein.

Mr. GREEN. OK, thank you, Mr. Chairman.

Mr. BRALEY. Would the Texas gentleman yield?

Mr. GREEN. Sure.

Mr. BRALEY. Mr. Chairman, Ms. Miller, a number of reports observed a culture within NNSA of prioritizing costs, cutting costs above the needs of security. As a follow-up to the question Mr. Barton asked, have M&O contractors throughout the complex been told to cut their security costs?

Ms. MILLER. They certainly have not been told to cut their security costs as any means of a policy, but I would say there is definitely messages that get communicated that when money is tight, people are looking for ways to cut costs and within an individual organization, a contractor organization are working with federal people, they may, as General Finan said, start to make decisions at very low levels on what their interpretation is of the need to cut costs.

Mr. BRALEY. So it sounds like they could have been cut, so as a follow-up, have security funding allocations been reduced in recent years before the incident?

Ms. MILLER. Security allocations have come down over the last several years, that is right.

Mr. BRALEY. Mr. Chairman, this is a concern I think that we had. Mr. Barton asked a similar question, and hopefully it is something that we can pursue. You know, I would be interested if security funding has been increased after the incident as well, but I think we will find that out later.

Thank you, Mr. Chairman.

Mr. GARDNER [presiding]. Thank you. Gentleman yields back.

Gentleman from Texas, Dr. Burgess, is recognized for 5 minutes.

Mr. BURGESS. Well on the GAO report that was supplied for this hearing, there is a table, table one on page nine of the report, and you know, it is interesting in light of the last question that was just asked about the funding levels. I mean, this is a comparison of a GAO study done in May of 2003 and then the security task force in February, 2013, so essentially a decade worth of NNSA oversight. And you look at the various things that are listed there, the last one being allocating staff. In 2003, the GAO found NNSA had shortfalls in its site offices in number and expertise of staff, which could make it more difficult for site offices to effectively oversee security activities. OK, that sounds like a real problem identified by the GAO. So what did General Finan find 10 years later? The NNSA security function is not properly organized or staffed. It sounds like the same problem to me, stated another way.

So you know, as interesting as this chart is, it really shows that the General Accountability Office's review of the NNSA security organization, when you look at it and go down the list and see the problems with defining clear roles and responsibilities, assessing site security activities, overseeing contractor activities, allocating staff in each and every case.

So General Finan, you know, it begs the question, it is almost every problem that was identified 10 years ago, you encountered on your task force 10 years later. So what do you think? Are these longstanding cultural problems that are ingrained in the organization, or are these things that can be corrected?

General FINAN. Clearly they are long-term cultural basic issues that need to be fixed. And what happens over the years, as we looked at each one of those, reports would come out and people

would check the box and say yes, I took care of the findings. What happened was people were nibbling around the edges, you know, they would put a body or two—oK, you have a shortage, so a body or two would change. You know, that would just create a shortage someplace else. They didn't ever stop and take a look at the overall system. How are we going to fix this long term? So by nibbling around the edges, instead of getting at the core issues, they just perpetuated the issues for a decade, and probably even longer than that, but every report that we looked at had striking similarities to what we found.

Mr. BURGESS. So let me just ask you this. This is a basic question. How is putting more money into a structurally deficient system, how is it going to make it better? I mean any amount of money—I agree that, you know, it is reasonable to look the funding levels, but for crying out loud, we have known about this stuff for 10 years and you haven't fixed it.

General FINAN. And fundamentally, you know, that is why I propose a change in the organization and change in the assessment model. Now I think that there are minor increases in budget that might be required, but we are not talking about, you know, hey, let's add a billion dollars to the security budget, because the issues that surfaced at Y–12 were structural within the organization and structural within the assessment model. Now there are other technical aspects of why the guard didn't respond properly, a whole bunch of things like that that are training related and things like that, but we are—when we are talking about the organizational structure, we are talking about some bodies. Yes, there is a shortage of security professionals, so you are talking a small number of additional bodies, and with the assessment model, you are talking about beefing up and changing the assessment model, but you are not talking about a massive influx of dollars.

Mr. BURGESS. Well, Chairman Upton in his opening statement said we need to learn the right lessons from past mistakes. I now certainly thank you for the effort that you have put into this. I just pray that 10 years from now another Congress is not having another hearing over the same sorts of failures.

So Secretary Poneman, let me ask you. Back in 2010, Chairman Emeritus Barton was ranking member. He and I wrote to the Secretary expressing our concerns that the safety and security reform initiative would weaken outsource by outsourcing safety and security. We requested the General Accountability Office to evaluate—actually Chairman Waxman, who was chairman at the time and Ranking Member DeGette did join in that letter, so given the troubled history of safety and security in the complex, NNSA's problems of implementing its own security program, what was the Department's justification for embarking on this project?

Mr. PONEMAN. It was clear at the time, Congressman, that we needed to focus, and you know the old saying, "If you don't know where you're going, any road will take you there." So when I arrived at the Department, there were many people saying many different things. We said let's sit down and figure out what are we doing to be safe, what are we doing to be secure? That was the genesis of that reform. Our management principles say we will only succeed by continuous improvement. This was part of that process

so it wouldn't just be mindlessly continuing to check the box, but being vigorous and aggressive and saying how do we be safe? I couldn't agree more with you, Congressman, in your premise that it ain't just throwing dollars at it, it is a deeply cultural thing, and that reform, which I know people have had some concerns about, was intended to be exactly part of the process that you are advocating in terms of a self-vigorous analytical process to get safe and to make people wake up, think, and be active about it.

Mr. BURGESS. Well, Mr. Chairman, I have got additional questions. I will submit those in writing. I thank you for the indulgence, and I will yield back.

Mr. GARDNER. Thank you. Gentleman yields back and the chair recognizes himself now for 5 minutes.

General Finan, a question to you. In your testimony, you write that the NNSA is structurally inadequate to address security needs. You have made your recommendations. What percentage of those recommendations have either been implemented or on their way to implementation? Just give me a number, if you could.

General FINAN. At the time I left the organization, all of the recommendations were in process of being implemented.

Mr. GARDNER. Thank you.

Additional questions to Ms. Miller, and this question was referenced earlier. The statement that Mr. Don Cook, NNSA Deputy Administrator for Defense Programs had made earlier, he said with regard to the relationship that we have and where we are between NNSA and its labs and plants, the statement was made "eyes on, hands off." And I think one of the concerns that we have is this isn't just about management; this is about leadership, a culture of safety and security. And I am very concerned when it comes to the approach that NNSA, when they talk about "eyes on, hands off," that this is actually a management style that is failing to provide the kind of leadership we need in safety and security. Would you agree or disagree with that?

Ms. MILLER. I think what is failing and what has failed is something I spoke a little bit about earlier, and that is it is one thing for people at a very senior level to talk at a very senior level and come out with phrases that they perfectly understand and they may be able to explain to the seven or eight people they talk to all the time about it. That is a very different thing if you are the person six, seven, eight layers down to understand what does that mean for the job you do every day?

Mr. GARDNER. And so you can see how that kind of creates a culture, though, that doesn't focus—that focuses more on management and less on leadership of a culture that is truly about safety and security.

Ms. MILLER. I think what happens is it leads everybody to focus whatever way they can to cope with what they think the person at the top is trying to tell them.

Mr. GARDNER. So what are you going to do to make that that is different?

Ms. MILLER. So as you know, right now I am acting administrator. What we have already begun in NNSA is a change in both the way we talk to staff and our contractors from the lower levels all the way up through the very top levels to be able to allow peo-

ple to understand how they do—how they are meant to do what they do in a safe and secure way, and to understand that safety and security is not the job of the people—it is not just the job of the people in the uniforms or the guys who can discuss criticality safety in depth, it is everybody's job. It is what you do every day as part of what else you do every day.

Mr. GARDNER. Recognize it is about the leadership, not just management.

Ms. MILLER. Absolutely.

Mr. GARDNER. General Finan, in your testimony, you talked about tension between security and the conduct of operations, stating that the events at Y–12 illustrate how far the pendulum has swung too far in the wrong direction, and that NNSA must clearly and consistently emphasize the importance of security. Do you believe the tension between security and operations is inescapable, or do you think that strong safety and security culture can facilitate improved operations performance, given committed leadership?

General FINAN. I absolutely believe that safety and security can make operations better, and depending on how they are integrated, you will have a better operation. But it is a cultural change and it is a difficult cultural change.

Mr. GARDNER. Is the agency right now on the way to that cultural change?

General FINAN. They are trying to make that cultural change. Again, it is a long term. It will take years and constant pressure, constant attention.

Mr. GARDNER. Adequate progress, in your mind?

General FINAN. They are making early steps. Early steps. It is going to take a long time.

Mr. GARDNER. But adequate process not quite ready to say that?

General FINAN. I am not quite ready to say that.

Mr. GARDNER. Ms. Miller, do you agree with General Finan that there has been a culture of compromise at NNSA?

Ms. MILLER. Yes.

Mr. GARDNER. And what are you doing to eliminate that culture?

Ms. MILLER. That is a culture that I think not intentionally, but definitely effectively, has permeated both the contractor and the federal side of it, and that is a question of leadership making clear what the expectations are for all concerned.

Mr. GARDNER. And you believe you have taken the sufficient steps so that your senior managers understand that there must be consistent messaging on security?

Ms. MILLER. I think through a number of actions that have been taken, including the shakeup in management of security, that message has been very clearly communicated as to what is expected of everyone.

Mr. GARDNER. And can you tell the committee today, all of us on the committee, that the head of defense programs, the head of the budget, the federal site managers, your managers, all are now singing from the same hymnal, so to speak?

Ms. MILLER. I can tell you that they know they better be. I can't swear for another person, but I believe it to be the case.

Mr. GARDNER. And have you committed—this information that you are talking about now, you have communicated it simply—sup-

ply the committee with memoranda or other communications instituting your policy for emphasizing that security?

Ms. MILLER. Yes.

Mr. GARDNER. Thank you. I appreciate your time, and with that, I don't see any other witnesses, so I will give the gavel back to the chairman.

Mr. MURPHY. Thank you.

We are going to dismiss this panel and move on to the next one. I do want to thank you all for your candid and thorough response, and this is extremely important to see leadership being honest with us. So we look forward to working with you more and talking with you more, and General, a special thanks to you for your report. Good luck over there, keep that Air Force in line. Thank you, ma'am.

We will wait for the next panel to come forward.

Ms. DEGETTE. Chairman, maybe we can just put her in charge of everything.

Mr. MURPHY. Well ma'am, I am Navy so we will have to discuss that.

Well, while this next panel is getting ready, I will start off by introducing them in the interest of time as we move forward. We have with us Mr. C. Donald Alston, Major General, United States Air Force (retired), and former commander of the 20th Air Force Global Strike Command, and Commander Task Force 214 U.S. Strategic Command, Francis E. Warren Air Force Base in Wyoming. We also have Mr. Richard Meserve—am I pronouncing that right, sir?

Mr. MESERVE. Meserve.

Mr. MURPHY. Meserve, thank you, President of the Carnegie Institution for Science, and former Chairman of the U.S. Nuclear Regulatory Commission from 1999 to 2003. We also have Mr. David Trimble, the Director of Natural Resources and Environment Team, Government Accountability Office. Welcome here today.

As you know, the testimony you are about to give is subject to Title XVIII Section 1001 of the United States Code. When holding an investigative hearing, this committee has a practice of taking testimony under oath. Do you have any objection to testifying under oath?

They all agree to testify. The chair then advises you that under the rules of the House and rules of the committee, you are entitled to be advised by counsel. Do you desire to be advised by counsel during your testimony today?

They all decline counsel.

In that case, if you would please rise, raise your right hand, and I will swear you in.

[Witnesses sworn.]

Mr. MURPHY. Thank you. I note for the record all the witnesses have answered in the affirmative.

You can now give a 5-minute summary of your written statement. We will start with you, Dr. Meserve.

TESTIMONY OF RICHARD A. MESERVE, PRESIDENT, CARNEGIE INSTITUTION FOR SCIENCE; C. DONALD ALSTON, MAJOR GENERAL, USAF (RETIRED); AND DAVID C. TRIMBLE, DIRECTOR, NATURAL RESOURCES AND ENVIRONMENT TEAM, GOVERNMENT ACCOUNTABILITY OFFICE

TESTIMONY OF RICHARD A. MESERVE

Mr. MESERVE. Mr. Chairman, Ranking Member DeGette, and members of the subcommittee, I am very pleased to appear before you this morning to testify of the security at DOE complex.

My involvement with this issue, and I believe General Alston's as well, arose as the result of a request that was made by Secretary Chu that we, as well as Dr. Norm Augustine, undertake an evaluation of basically the structure for the management of security at DOE. We undertook a study that involved visiting sites, reviewing documents, interviewing people, and as a result of all of that effort, we submitted three separate letters to the Secretary on December 6 of 2012, and we have submitted copies of those letters for the record as our testimony.

We did not purport to investigate the factual circumstances surrounding the Y–12 institute. Our reports focused on management-related issues, and I hasten to add that our report was a snapshot in time. I was learning a lot about what has happened at DOE since we conducted our interview from the very informative testimony that we have all benefitted from earlier this morning.

There are a couple of points from my letter that I think I would like to emphasize that I see as clear issues that DOE should confront. I believed that on December 6, and I believe they are confronting them. One, and I think a critical one, is to make sure you have a management structure in place that assigns clear authority and responsibility for security. One of the underlying factors at the Y–12 incident is there was a division of responsibility and without anyone being truly in charge until you had a situation with a contractor responsible for the guards and a different contractor responsible for the security-related equipment and the cameras, and they weren't communicating well and a lot of the equipment was out of service and each could point at the other.

I also came to the conclusion—and I will let General Alston speak for himself—that the federal oversight needed to be improved. It was—serious security issues existed before this episode and no one at DOE that we saw was really on top of detecting them and correcting them.

There was issues associated with the protective force, ensuring appropriate training. There was an issue associated with the, obviously, the behavior of the first responder. There were many issues associated with the protective force that need to be addressed. We need to find a clear trajectory for these people. We need to make sure that they have a sense that they are an important part of the team and integrated with the team.

I think that all of us came to the view—and this has been emphasized this morning—that one of the things needs to change is the culture. There has to be a security culture that places both safety and security as highest priorities, and that management by its word and deed reinforces that, and that everyone at the site re-

alizes that it is their individual responsibility to assure security, and that clearly is something that has been failing.

And finally, I think what I would add is a need for balance. Clearly, this episode reflected issues associated with physical security, but there are other security issues that confront the Department, and in order to recognize, you need a balance. There are cybersecurity issues, there are personnel security issues, all of which need to be functioning, and one ought to not, because it was an episode of physical security, focus solely on that.

My views are explained more fully in the letter that was submitted as part of the record, and I welcome the opportunity to talk to you this morning.

Mr. MURPHY. Thank you. General, I promised you I would have you go first. I apologize for the confusion there, but you are recognized now for your opening statement.

TESTIMONY OF C. DONALD ALSTON

General ALSTON. Mr. Chairman, Ranking Member DeGette, members of the subcommittee, I would only briefly amplify what my colleague has so well described as Mr. Augustine's, Dr. Meserve's, and my efforts on behalf of Dr. Chu and the Department of Energy. I would only amplify one particular point, and that would be the culture piece.

We have talked this morning—the first panel engaged you in conversation using some of the expressions that we found to be of concern, "eyes on, hands off" for example, and that expression is something that came out of just the last couple years of policy changes. But as has been reinforced over and over again, the recurring challenges, the similar recurring challenges, go beyond the "eyes on, hands off" policy emphasis that had occurred over the last years, and I think that at the center of the challenge for the Department is the cultural change. And one aspect of the cultural change that is—that feeds the cultural challenges is the distributed management, the way the Department distributes its management across its labs, and the labs prefer and are very successful in their pursuit of the distance between the headquarters and the labs themselves, and the freedom of movement that they have, and this has great value, I would concede, on the science piece, but I think that that contributes—the security, in fact, needs to have more central—management central emphasis, common standards, and what I have observed is that you see people talk about mission, which I read as science. People talk about safety, and there is more of a pervasive safety culture, if you will. But security is not everybody's responsibility, and it is as if mission, safety, and security are in a trade space where when there is an emphasis on security because of an episodic failure, the other elements of mission and safety see the focus on safety as to be marginally at the expense of the other parts of the mission, as opposed to looking at it as an enterprise challenge, and that, in fact, they don't share trade space with each other, but in fact, are all essential every day to mission success.

And with that, I thank the committee for the opportunity to have dialogue this morning.

[The joint prepared statement of General Alston and Mr. Meserve follows:]

Statement before the U.S. House of Representatives Committee on Energy and Commerce

Subcommittee on Oversight and Investigations

Hearing on

DOE Management and Oversight of Its Nuclear Weapons Complex: Lessons of the Y-12 Security Failure

Joint Statement
by

C. Donald Alston
Major General, USAF (retired)

and

Richard A. Meserve
President, Carnegie Institution for Science

March 13, 2013

Rayburn House Office Building Room 2322

Mr. Chairman, Ranking Member Diana DeGette, and members of the subcommittee, we thank you for the opportunity to appear before you today.

With the subcommittee's permission, we would like to submit as our statement three separate letters authored by Mr. Norman Augustine and ourselves. These letters were submitted to Secretary of Energy Stephen Chu concerning the management of physical security at the Department of Energy Category 1 nuclear facilities. In October 2012, Secretary Chu asked the three of us to consider a variety of management models and to provide separate, individual observations regarding management structures that might be appropriate for application across Department of Energy and, specifically, National Nuclear Security Administration sites. We provided our respective letters to Secretary Chu on December 6th of last year.

We would like to provide some context about our assessments. While Secretary Chu did not ask us to investigate the Y12 security breach, we used that incident and resulting investigations as an entry point into a larger examination of the management system. Additionally, we were exposed to draft corrective actions resulting from those investigations, but we did not evaluate these measures or their implementation across Department of Energy and the National Nuclear Security Administration. Finally, our written assessments were informed by our direct engagement during a brief seven-week period last fall, culminating in early December. We are not up to date with regard to any changes that have been introduced. Nonetheless, we hope that our observations are helpful to you.

Thank you for the opportunity to appear today before the subcommittee, and we welcome your comments and questions.

C. Donald Alston
1515 North Star Loop
Cheyenne, WY 82009
December 6, 2012

The Honorable Steven Chu
Secretary of Energy
U.S Department of Energy
1000 Independence Avenue, SW
Washington, DC 20585

Dear Secretary Chu:

In light of the perimeter security breach at the Y-12 National Security Complex (Y-12) in July 2012, you asked me to examine a variety of organizational constructs for physical security and to provide you with observations on the value of transitioning to a common model.

My observations have been informed by reviewing the considerable body of work that has been done on this subject over the past decades; through interviews and discussions with current and former DOE leaders, as well as experienced leaders outside of DOE; and by a number of site visits. I was able to visit DOE headquarters (HQ), Y-12, Pantex Plant, Sandia National Laboratories, Los Alamos National Laboratory, Savannah River Site, and the Calvert Cliffs commercial nuclear power plant in Lusby, MD. The site visits enabled discussion with maintenance and operations (M&O) contractors, DOE overseers, and protective force management and members, including union leaders. A very candid exchange at all levels with dedicated, experienced professionals greatly aided the effort.

Four physical security organizational models were reviewed: 1) a proprietary protective force organic to the M&O contractor responsible for site operation; 2) a protective force subcontracted to the M&O contractor; 3) a federalized protective force; and 4) U.S. military forces. Three of these four models are currently functioning within DOE/National Nuclear Security Administration (NNSA); however, none of the four emerges as attractive long term, department-wide option without addressing systemic impediments that preclude effective change.

On the grandest scale, there were indications that security was viewed as the responsibility of the protective forces alone rather than as the responsibility of each member of the work force. While this culture may not be widespread throughout the DOE complex, it is clear that leadership could further emphasize the need to view security of our nation"s sensitive nuclear materials as a shared commitment across the work force. The Department of Energy is responsible for America"s nuclear enterprise, and enterprise credibility is derived from the trust and confidence our citizens, national leadership, friends, and allies have in the Department"s ability to maintain a safe, secure and effective U.S. nuclear weapons complex. Importantly, this credibility factors into the daily calculus of potential adversaries and contributes directly to achieving an effective deterrent posture, a commodity re-earned every single day. A pervasive culture in which each member of the nation"s nuclear weapons complex recognizes the vital role he/she plays in assuring both security and safety contributes directly to maintaining that credibility.

As currently structured, no recognizable critical path exists between DOE HQ and the site security organizations to ensure daily security success. Study of a variety of DOE and NNSA

This updated version (dated December 10th) of the original letter contains minor clarifying edits.

organizational charts could not demystify where authority lies. The Department struggled to articulate how information flows – both up and down – between the sites and DOE HQ and could not easily provide a depiction of that process. I think this environment contributes to the reality that nuclear material at Savannah River Site – which falls under DOE"s Environmental Management (EM) office – can be secured with different standards and policies than those required at NNSA sites. The category of material should drive security requirements, not the organizational chart.

Distance has been growing between the headquarters and the sites, a trend that follows a DOE legacy of decentralized management across its facilities. While this traditional arrangement may pay dividends for the department in many respects, security is not one of them. Recent efforts to revise DOE"s safety and security directives and modify the department"s oversight approach to provide contractors with the flexibility to tailor and implement safety and security programs without excessive federal oversight or overly prescriptive departmental requirements, as well as NNSA"s "governance transformation" that increased reliance on contractor"s self-oversight through its contractor assurance systems, have fortified sites" sense of independence and distance from the HQ. Sites leverage their unique missions and geography to justify a preferred "alone and unafraid" mantra, and the HQ has employed a largely "hands off" response.

Mutual distrust is bred as HQ personnel in key security roles are viewed as inexperienced regarding security matters and too far removed from the site to understand the uniqueness of local challenges. Key leaders must have credible security experience -- especially since there is little to no assignment circulation of security personnel to and from the HQ; no missionaries emerge to bridge the gaps in trust.

What little leverage the HQ has comes in the form of additional inspections and assessments – "black hat" interactions that further contribute to adversarial relationships. Inspection is an absolutely essential tool to validate compliance and operational readiness. However, it should be one dimension of a composite assessment process. Depending too much on snapshot assessments and not developing the right metrics to measure daily readiness would provide leadership little satisfaction regarding the true state of security preparedness and program execution.

Further, there is a perception that corporate security policy is being written from inspection results. If true, the Department risks drifting from measuring original standards to an environment where sites lack confidence in the integrity of the inspection process as they perceive they are chasing the latest inspection results. In the DOE/NNSA HQ construct, a dynamic or volatile policy environment led by DOE"s Office of Health, Safety, and Security (HSS) risks marginalizing NNSA security responsibilities. Of course, even if these site perceptions are inaccurate, leadership needs to be sensitive to these atmospherics.

Communication is an area ripe with opportunity. Given today"s environment where sites seem to prefer to operate independently, where there is no effective best practice/lessons learned dialogue between sites, no program for security information exchange with the Department of Defense (DoD) or commercial nuclear activities, it is not surprising that site facility staffs can and do conceive, design, develop, test and deploy modifications to security systems. To better understand and share risks associated with changes to security systems there could be a normalized process over watched by DOE HQ, leveraging a revitalized Sandia expert review, with hard requirements for developmental and

operational testing and red teaming that could methodically deliver security modifications ready on day one.

In my final analysis, the NNSA Administrator must always be able to answer the following questions:

- How ready are we today and how do we know?
- How ready will we be in 6 months and how do we know?

A variety of sources produce the set of ingredients that create the mosaic of indicators conveying the current and future state of the security program. Timely, balanced reporting, where good news travels fast and bad news faster, not only provides content, but also serves as a barometer for the quality of the self-critical culture. Quality metrics that provide both tactical and operational level content, deliver today"s picture and, measured over time, expose trends and opportunities for course corrections. Collaboratively developed metrics, together with processes that actively seek input where appropriate on policies and standards also builds trust. Checks and balances in development of new or improved security capabilities, to include external review processes, provide corporate-wide awareness and ensures sites have support during transitions. A comprehensive human capital development program creates career paths at all levels and could provide for circulation up and down the chain, all the while driving greater security competency across the enterprise.

Based on discussions over the past two months, the attributes of the objective security organizational construct should include:

1) A force with a mission focus that understands the vital interdependencies and coordination required at all times with the M&O contractor;

2) A well-trained, disciplined force whose professional conduct during routine operations is dependable and above reproach and one that is prepared to use lethal force if required during emergency operations;

3) A force conditioned and incentivized by leaders at all levels to provide timely reporting;

4) A force that would help drive crosstalk across DOE sites, outside the department such as with the DoD, and with commercial nuclear businesses to benefit from others" lessons learned;

5) A force with an absolute intolerance for compensating for shortfalls/deficiencies/outages one minute longer than necessary;

6) A force that knows - based on facts -- how ready it is today and leaders who know how ready it will be 6 months from now;

7) A force not remotely prone to work stoppage as a job action; and

8) A force that understands the merits of centralized control and decentralized execution of security responsibilities.

Of all the candidate security organizational models I examined, the military model is the least attractive to me to meet DOE/NNSA needs. The advantages include a dependable, high-quality, rotating force that would routinely be refreshed to meet mission demands of a typically non-dynamic environment. However, the lack of continuity would produce a force less familiar with the site than other models, and transitory leadership will have to adapt to a relatively unfamiliar mission (enriching uranium, for example). The most significant disadvantage is the division of unity of command by the introduction of a substantial command and control seam between protective forces and site operations with the arrival of Department of Defense onto the DOE/NNSA playing field. Would there be any risk that geostrategic instabilities might make these war fighting forces the first to be redeployed abroad, driving challenging domestic security contingency plans? I do not see an effective role for a DOE/NNSA representative in this model.

The proprietary guard force, which has security personnel organic to the M&O contractor operating the site, provides the cleanest unity of command option. The risk of security work stoppage seems less likely in this model than other contractor options. Poor performers can be removed with ease. The drawback to this option is the uncertain security competencies of potential M&O contractors. This model is a variation on the status quo where a DOE/NNSA security representative provides oversight of the security elements of the M&O contract.

The model in which the protective forces are part of a company subcontracted to the M&O contractor has a mixed record. There is a history of work stoppage. There is a manageable seam as far as unity of command is concerned. History shows this model can provide a disciplined, professional force with valuable continuity and familiarity with the site. (I would note here that military experience probably makes up between 50 and 75% of the force, though most of those veterans have no nuclear security experience upon arrival. Good orientation and training programs make up for this significant deficiency and ensure those with and without military experience are prepared to provide effective security.) At Y-12, the maintenance function was not owned by the protective force which may have contributed to improperly prioritized maintenance of security gear, which ultimately resulted in failure. Overcome this specific contract deficiency and this model will present less risk than it currently does. This model is a variation on the status quo where a DOE/NNSA security representative provides oversight of contract execution by the sub-contractor.

The model I find the most attractive is the federal model. It is proven, working effectively in the DOE/NNSA transportation business providing for a disciplined professional force. It precludes work stoppage risk. True, adverse actions are less swift than the contractor models and this approach does introduce a seam with the M&O contractor. However, this model is a substantial departure from the status quo and what you trade in local unity of command you gain in more effective corporate oversight of security operations. I see the role of the DOE/NNSA security representative as the leader of the site security forces and the key integrator with the M&O leadership. The long term culture shift this model could drive should be weighed positively in an organizational change decision.

For your consideration, Admiral Mies oversaw an in-depth study of DOE security in April 2005, "NNSA Security: An Independent Review." I think a hard-hitting, „show me" re-assessment of the status of his recommendations would benchmark the state of your self-critical culture and prove very helpful to the Department.

All members of your Department rapidly responded to requests for information and made time for discussions at my convenience. Everyone I met, both the contractors and Department personnel, were forthright, professional, and dedicated to mission success.

I am honored you asked me to support this important project. Thank you. It was a great experience working with the men and women of your Department. And thank you for providing the support of the talented members of Center for Strategic and International Studies. I could not have produced this work without their tireless support.

With great respect,

C. DONALD ALSTON

This updated version (dated December 10th) of the original letter contains minor clarifying edits.

NORMAN R. AUGUSTINE
6801 Rockledge Drive
Bethesda, MD 20817
Tel. 301-897-6185 Fax 301-897-6028
norm.augustine@lmco.com

December 6, 2012

The Honorable Steven Chu
Secretary of Energy
U.S. Department of Energy
1000 Independence Avenue, SW
Washington, DC 20585

Dear Mr. Secretary:

This letter responds to your request that I assess certain physical security shortcomings experienced by the Department of Energy (DoE), most prominently at the Y-12 National Security Complex (Y-12), and provide observations, findings and recommendations.

Given the relative short amount of time available for this review, my recommendations are more in the form of suggestions; however, they are based on over a half-century of managing at all levels in large organizations. I have drawn upon lessons gained during the ten years I devoted to government service, including several years as Under Secretary of the Army, and a number of years as CEO of an organization with over 180,000 employees, many working on sensitive national security systems. Further, in keeping with your request, I have been extremely candid in my assessments, which in no way suggests any diminishment in my overall respect for the people who are charged with such enormous responsibilities as are those in your Department.

Although this letter is no doubt considerably longer than you intended, the matter at hand is in many respects a complex one, and its importance obviously merits careful consideration. This document has been prepared at the unclassified level for your convenience; however, I would be pleased to provide further substantiation and clarification of various issues at a higher level of security, should you wish.

I would note at the outset that I am highly indebted to the people working in the Department of Energy, who were generous with their time and expertise and were extremely forthcoming, even welcoming, in sharing their views on what are often controversial issues. A particular debt of gratitude is owed to the staff of CSIS that supported us; they are a group of professionals.

This updated version (dated December 10th) of the original letter contains minor clarifying edits.

APPROACH

In conducting this review, I have read on the order of 1,000 pages of documents, some at classified levels, and held discussions with literally dozens of individuals, both management and non-management—the latter in some cases without management present. I visited Y-12, Pantex Plant, Sandia National Laboratories, Savannah River Site, DoE headquarters, and the Calvert Cliffs nuclear power generation plant. (The reason for conducting the field visits was to benefit first-hand from examining the different management models they embrace; to search for systemic problems; and to assure the degree of thoroughness that the task you assigned deserves.)

The mindset you will hopefully find reflected in this letter is one commensurate with DoE's extraordinary responsibility of, among other things, providing for the security of sensitive nuclear materials and weapons. Failures in this arena can, as you know so well, directly impact the lives of millions of people as well as reshape the world's geopolitical landscape virtually overnight. Under such circumstances, there can be zero margin for error, and that is the attitude that has been adopted in conducting this review.

OVERALL FINDINGS

"Unacceptable and inexcusable" were the words aptly used by the Administrator of the National Nuclear Security Administration (NNSA) testifying before the Congress with regard to the events of July 28 at Oak Ridge; as you know, three individuals, one an 82-year-old nun, penetrated four fences and several clear-zones during the night, and when finally confronted, these individuals faced a trained security officer who acted principally as a spectator. Disconcertingly, I can see little reason why, under the specific prevailing circumstances, the intruding group could not have included, in addition to the three persons actually participating in the incursion, a well-armed follow-up group. I must disclose that I have been involved in dozens of failure analyses of a variety of types during my career, and none has been more difficult for me to comprehend than this one.

Many security professionals with whom we spoke reacted to the Y-12 incident with extreme embarrassment and, as in my own case, perplexity. The overwhelming majority of these individuals are very proud of the work they perform and are generally aware of the importance of their mission...which makes the cascade of failures that led to the events of July 28 all the more enigmatic.

You asked that I address the pros and cons of various management structures that would better serve the Department in providing physical security, and I have done so. While this is important indeed, I conclude that, rather convincingly, the management structure was an abetting, not a root cause, of the problems encountered on July 28. The fundamental

This updated version (dated December 10th) of the original letter contains minor clarifying edits.

problem was one of culture: a pervasive culture of tolerating the intolerable and accepting the unacceptable.

As examples of this culture, a false alarm rate surpassing by orders of magnitude anything that I have ever encountered before was accepted as a fact of life. When full-time surveillance cameras failed, a "compensatory measure" was introduced that consisted of (relatively infrequent) periodic patrols. Word of no-notice tests was leaked to those security forces being tested. Failed security systems went unrepaired for months (yet were repaired within days after the Y-12 incursion when attention was focused upon the issue). There was cheating on proficiency exams. "Tune-up" firing was permitted prior to marksmanship qualification tests. Worthiness tests of hardware were delayed until the hardware was in working condition on the grounds that there is no sense testing hardware that isn't working. Strikes of the guard force were largely dismissed as being readily offset by substitute guards (even though we were told that as many as three sites have entered union negotiations at about the same time, which could limit the availability of such substitutes).

The demands of securing nuclear materials, components, and devices are perhaps of unmatched unforgiveness—yet in general it is an endeavor of chilling monotony. Individual security personnel can (hopefully) expect that they will never confront a true threat during their entire career. Add to this the hundreds of false and nuisance alarms that occurred (and occur) each month—and then working 12-hour shifts (albeit some involving rotation)—and one has a mind-numbing challenge even for the most dedicated professional. (Regarding the length of shifts, as explained in one DoE report, the workforce likes the overtime pay and days off.)

The various corrective action plans and numerous security reviews (going back to 1986) reveal a pattern of inverted priorities, to wit, from highest to lowest:

1. Accommodate the workforce.
2. Reduce costs.
3. Secure nuclear materials, components and devices.

In summary, the problem the Department faces within the context of this review is a culture of permissiveness, amplified by the absence of day-to-day accountability and exacerbated, in the case of Y-12, by an ineffectual governance structure.

As will be discussed later, I favor the Federalized Force model for a number of reasons. However, if this cannot, for various reasons, be implemented, I believe that the single-contract ("new" Y-12) model can be made to work...as could another alternative I will offer.

This updated version (dated December 10th) of the original letter contains minor clarifying edits.

Unfortunately, one of the most difficult things to change is a failed culture. My observations over the years have, however, convinced me that change can be introduced and that there are at least seven ingredients to successfully do so:

1. Make sweeping changes...begin with a "clean sheet of paper"—simply "trying harder" to do what you have been trying to do all along is a formula for failure.
2. Make leadership changes wherever doubts exist as to its effectiveness.
3. Devote a great deal of effort to communicating the new culture.
4. Be intolerant of even the slightest reversions to the old culture.
5. Lead by example—demand that all in leadership positions *"walk the talk."*
6. Execute change fast...prolonging change so that everyone can get used to the new system is self-defeating.
7. Weed out individuals who cannot accept the new culture (Vince Lombardi: "If you are not fired with enthusiasm you will be fired with enthusiasm!")

CAUSAL FACTORS (Y-12)

The following six factors seemed to predominate as triggers for the Y-12 incident of July 28 (note: one earlier assessment identified 26 specific factors that contributed to the security failures):

Failure of Early Warning System. Numerous reviews of Y-12 physical security have been conducted over the years; however, none—including one by NNSA not long before the July 28 incident—expressed extraordinary concerns, although several cited troublesome indicators. In the case of the line-management system, the headquarters relied upon the site management; the site management relied upon the two primary contractors; and one of the two primary contractors was facing a competition and the union was concerned with an upcoming contract negotiation. In short, bad news did not flow upward, having been underappreciated or filtered at every level. The speed of light exceeds the speed of dark!

Lack of Systems Approach. Razor (or concertina) wire was in place around part of the Y-12 perimeter...but not all. There was no evidence of a disciplined analysis of single-point or even multi-point failure modes. DoE sites, for example, have far fewer cameras than does the Calvert Cliffs power plant. It was reported that sixty compensatory measures were in place at Y-12 to "offset" malfunctions, but from a systems standpoint many of them were not truly compensatory. When the necessary funding to implement the ARGUS security system was not forthcoming (by nearly a factor of four), ARGUS was mated to elements of the existing system without adequate systems testing—and then rushed into

operation—apparently without objection by the Site Office. The result was that the "system upgrade" actually deteriorated system performance.

Split Responsibilities. Wackenhut Services, Inc. (WSI) was responsible for the security force but the management and operations (M&O) contractor was responsible for the sensing, analysis, and display equipment. The Site Office appears to have withdrawn from its oversight responsibilities, having misinterpreted headquarters instructions as to its role. The role of a Site Office (or headquarters) with regard to contracted activities is not to manage those activities but rather to ensure that those activities are managed. At Savannah River Site, physical control of category 1 materials located at two proximate sites is currently overseen via two different chains of command emanating from DoE headquarters.

Focus of Inspection/Testing on Compliance. In general, inspections and testing have focused on verifying that contract terms are satisfied or that the Design Basis Threat (DBT) has been countered. Immense volumes of documentation containing innumerable check-lists have been produced—little of which addresses what the Department of Defense would consider Operational Testing (as opposed to Developmental Testing). Stated differently, tests have too often addressed the question, "Does the hardware or practice meet the design criteria rather than is it operationally effective?" Standards are often procedural rather than performance-oriented, and stress testing has been lacking. What is needed is not more inspections but better inspections.

Compartmentalization of Responsibility. During the review team's visit to the Calvert Cliffs nuclear power plant it was emphasized that if, for example, a member of the security force noticed that a production machine sounded differently from what they normally heard they would view it as their responsibility to report this observation. Further, it was the clear responsibility of management to run the apparent anomaly to ground and to report their overall findings to the security officer initially reporting the issues. This is in stark contrast to what occurred at Y-12.

The fact that certain sensors at Y-12 had been designated as priority 2 for repair should not have been an excuse for a very large number of sensors remaining inoperable for months, particularly when the problem was not elevated within the management structure, particularly including the Site Office, for resolution.

During visits to the previously listed sites, one heard complaints about persistent escapements (deficiencies) that were known and accepted because "That belongs to the M&O contractor," "It is part of the union agreement," "It is required by the contract," "The FAA wouldn't like it," "You can't cut down trees," etc. It is critically important that all escapements be identified and reported, resolution responsibility assigned, root causes found, corrections introduced and tested, and open-items formally closed. (In this regard,

NASA and its contractors have evolved highly effective systems in support of the human spaceflight program that might be conceptually helpful to the DoE.)

Lack of Independent Verification. Testing and auditing ultimately requires independence from those responsible for what is being examined. At some point these two functions obviously must come together in the chain of command; however, in general, the higher that coincidence takes place, the better. This is particularly true of operational (performance) testing that may involve off-nominal conditions.

The key individuals involved in such independent oversight need to be rotated periodically, much as audit firms are required to rotate account managers or the NRC rotates its field personnel. Absent this, the site offices can become relatively passive and increasingly insular. Site managers must be granted significant authority (and accountability) over work performed by contractors—not to give detailed instructions regarding work execution but rather to assure that contractor responsibilities are being met. Similarly, headquarters personnel should not seek to involve themselves in the actual execution of routine work, but should use their full authority to ensure that significant work is in fact properly executed. In short, micromanagement on the one hand and passivity on the other are not the only options.

MANAGEMENT PRINCIPLES

The suggestions that follow are driven by twelve management principles that I have discerned over my career (some the hard way!). These are as follows:

1. Recognize that management is all about people. Selfless, competent, committed, ethical leadership-by-example is the coin of the realm.
2. Focus on the primacy of mission.
3. Communicate expectations and listen to concerns. Establish a single chain of responsibility and provide commensurate authority and resources.
4. Maintain clear—and minimal—interfaces (both technical and organizational).
5. Assure accountability and enforce consequences.
6. Disproportionately reward significant contributors and do not endure under-contributors.
7. Analyze every escapement—no matter how trivial—to determine root cause, introduce appropriate corrections, and conduct confirmatory tests. ("There is no such thing as a random failure.")
8. Provide independent checks and balances.

This updated version (dated December 10th) of the original letter contains minor clarifying edits.

9. Maintain parallel channels for surfacing bad news (line management, auditors, ethics officers, suggestion boxes, etc.).
10. Culture can be an asset but it can never be an excuse.
11. Treat all persons with respect.
12. Operate ethically at all times.

Quality personnel can make up for an inadequate organizational structure, but a quality organizational structure can never make up for inadequate personnel.

ALTERNATIVE MANAGEMENT STRUCTURES

The myriad possible governance and management structures can conveniently be grouped into five basic models or hybrids thereof. Each has its advantages and disadvantages and, interestingly, three of the five are currently in use by the DoE, thereby offering first-hand experiential prototypes. These models are (a) Dedicated Physical Security—Military; (b) Dedicated Physical Security—Civilian; (c) Separate Operations and Physical Security; (d) Separate Operations and Full-Service Security; and (e) Integrated Operations and Physical Security.

(a) *Dedicated Physical Security—Military (Department of Defense (DoD))*
This model has the advantage of resolving protective force career issues, promoting strong discipline and providing a single, established chain of command. It suffers from coordination issues that may arise between two major government departments (DoE/DoD), rapid turnover of personnel, and a visibly expanded operational role of the uniformed military within the United States. Furthermore, assigning such a mission to DoD, even given its importance, would inevitably be viewed as a distraction from the Department's primary mission—a mission that is already extremely strained due to growing resource limitations.

(b) *Dedicated Physical Security—Civilian (DoE Office of Secure Transportation - OST)* The option of a federalized physical security force would virtually eliminate concerns over work stoppages, increase continuity, and offer a clear and highly focused chain of command. It also recognizes the paramilitary—as opposed to civilian—nature of defending nuclear assets. However, it poses career management challenges for the members of the force as they age, and it has been asserted that it could be more costly than some other options. This approach represents a transformational change that should promote creating a new culture; however, it would be very difficult to "unwind" if it should later be desired to do so. (Under this model it is important that the Dedicated Physical Security Force have an integral capability to install and maintain all security systems as well as to access

organizations capable of developing such systems so that interface issues similar to those encountered at Y-12 are to be precluded.)

(c) *Separate Operations and Physical Security ("old" Y-12))*
This model can produce significant potential interface challenges (between the M&O contractor and the security contractor) because of split responsibilities and reporting chains. It is also subject to work stoppages. On the other hand, it offers the advantage of a direct relationship between the Site Office and the critically important physical security contractor and greatly eases the problem of removing non-performing individuals and organizations.

(d) *Separate Operations and Full-Service Physical Security (new model)*
The primary failing of the Separate Operations and Physical Security model that was previously in place at Y-12 is its split of responsibility between two contractors for the performance of the physical security function. A workable excursion from this model that would maintain the needed emphasis on physical security professionals who are directly aligned with the Site Office would be to have separate M&O and physical security contractors *but with the latter having a "full-service" responsibility.* That is, the security contractor would be responsible not only for providing the Pro-Force but also for acquiring, installing and maintaining all security systems and other necessary equipment—directly overseen by the Site Office. In other words, rather than moving the Pro-Force to the M&O contractor, move that part of the M&O contract related to physical security to the security contractor. This would likely exacerbate relationships between operating employees and security employees but would provide a strong physical security capability and would remove physical security responsibilities from the M&O contractor that is more likely to be familiar with science or operations than physical security.

(e) *Integrated Operations and Physical Security ("new" Y-12, Pantex)*
At the M&O level, this model unifies responsibilities for security and operations and provides the site office with a single point of contact. It also permits rapid resolution of personnel and major contractor issues. It suffers from the possibility of work stoppages and demands that the M&O organization and its senior members assume a breadth of responsibility that spans from plant operations to maintenance to cyber security to physical security and much more. Most potential M&O contractors will not be versed in the demands of providing physical security. The formation of joint ventures alleviates this problem but does not eliminate it. In the case of sites focused on research and development it confronts the challenge of integrating the open culture of science with the closed culture of security. Particularly in time of crisis the M&O contractor, security contractor and Site Office will need to maintain close coordination; however, this is not unique to this

particular model since in all cases under such circumstances operational command shifts to the Pro-Force, with other organizations assuming a supporting role.

SUGGESTIONS

Given that no single model seems to offer a perfect solution, I would rank the five principal options, from best to worst, as follows, with the fourth of these being undesirable and the fifth being unacceptable (note that the second and third of these options would be considerably more attractive were it possible to obtain a federal ruling/law that precluded strikes by employees of commercial firms charged with securing Category 1 sites):

- Dedicated Physical Security—Civilian ("Federalized")
- Separate Operations and Full-Service Physical Security ("New Model")
- Integrated Operations and Physical Security ("Proprietary"—"New" Y-12)
- Separate Operations and Physical Security ("Old" Y-12)
- Dedicated Physical Security—Military (DoD)

The above ranking is, curiously, somewhat contrary to my confessed personal prejudices—that is, believing that the Free Enterprise System does work and that government should perform only those functions that the private sector cannot, or will not, perform (there are of course a number of such functions). However, in the case at hand, an overriding consideration is that the DoE is concerned with one of the most consequential missions in the world; furthermore, it is a paramilitary mission potentially entailing the use of deadly force. Such a mission is best executed with a singular focus and with the greatest possible authority.

The notion that individuals under some other models, many of whom have served our country in combat, would abandon their posts in a work stoppage while protecting a Category-1 site is, frankly, incomprehensible to me. Whatever the case, the federalized model largely negates that happenstance. I discount the rather widely-held view that such eventualities are readily handled through backup plans, and do so in part because of the possibility that (as has recently occurred) multiple union contracts could expire at about the same time. (Note that work stoppages become a possibility even when union contracts contain no-strike provisions *if that contract is no longer operative due to its expiration.*)

It is again emphasized that the Dedicated Physical Security—Civilian model must be a "total package" solution and include an integral capability to obtain and maintain all necessary physical security devices and equipment.

There are at least two major disadvantages to this overall approach. First, it poses non-trivial challenges in workforce career management. Second, any attempt to implement it is likely to confront enormous opposition. With regard to the former, it is noted that there

This updated version (dated December 10th) of the original letter contains minor clarifying edits.

are many government jobs (as well as M&O contractor jobs) that security force members can fill when they are no longer capable of meeting the high physical standards demanded when assuring nuclear security. Further, during the review, few if any instances were found where such problems have been significant (under any of the models in use). With regard to the latter concern, it is simply noted that the issue at hand has to do with the security of nuclear materials and weapons. Enough said!

If, however, for any reason it is not practicable to implement the Dedicated Physical Security—Civilian model, the Separate Operations and Full-Service Physical Security model or the Integrated Operations and Physical Security model, the latter as used at Pantex and has been introduced at Y-12 following the July 28 event, should be workable. The Integrated Operations and Physical Security model could involve either a single contractor or a joint venture. Both options offer the distinct advantage of making necessary corrective actions regarding personnel far more expedient than the preferred approach cited above. (In my experience, I have found the government personnel system to be far more tolerant of [the relatively rare cases of] clearly substandard individual performance than the civilian sector.)

The DoE is currently in the rather awkward situation of having (appropriately) abandoned as unworkable the Separate Operations and Physical Security model at Y-12, yet continuing to preserve that same model at the Savannah River Site (SRS)—with exactly the same security contractor! In discussions with the leadership of SRS it was clear that they are uniformly confident of the suitability and effectiveness of the existing situation. Based upon a one-day visit I would be hesitant to question that judgment since, as repeatedly observed herein, given capable people almost any model can be made to work. However, I would *strongly* emphasize that some models are markedly more vulnerable to problems than others. It is my view that the Separate Operating and Physical Security structure is such a model.

Other related actions that I would commend for your consideration are:

- Establish a separate, dedicated organization responsible for conducting physical security (only) inspections and audits that reports directly to the Secretary of Energy (or, alternatively, the Nuclear Regulatory Commission). Field Sites would be responsible for periodically reporting status of all security elements to this organization.
- Reinforce the authority of Field Sites and Field Offices—nonetheless making clear that during actual physical security incidents the chain of command is entirely within the physical security management structure and that Site office responsibility is not to manage work but to assure that work is managed. If the Site Offices are present merely to observe, then it is not apparent why they are present.

This updated version (dated December 10th) of the original letter contains minor clarifying edits.

- Rotate select individuals between Headquarters and field sites in order to enhance understanding of the distinct roles, challenges and responsibilities faced by these two institutions (as is commonplace in industry) and thereby increase overall effectiveness. This will require revisions to the existing DoE policies for reimbursing the cost of employee moves.
- Place security forces on eight-hour shifts. This would have the secondary benefit of producing a larger Pro-Force pool. (This is undoubtedly a strike issue.)
- Create a single office (at Sandia or Livermore) to develop standards and procurement guidance along with advanced equipment for security systems (biometrics, high resolution displays, animal-discriminating sensors, etc.). These standardized systems can then be tailored, *by exception*, to the particular local conditions of individual sites. (It is noteworthy that not all such solutions need to be high-tech. For example, Savannah River Site has implemented what appears to be a very effective rip-rap barrier, yet it is not in evidence elsewhere (excluding the Calvert Cliffs nuclear power plant where it is fully embraced). The use of dogs is another such example.
- Review the current threat model (which is said to be five years old). Involve outside organizations from both the intelligence community and the special ops community to participate in this effort.
- Re-balance responsibilities among NNSA and other DoE headquarters entities to assure that field elements operating under similar circumstances are provided with a single, consistent chain of command and set of procedures. The creation of the reporting relationship of the Field Sites to NA-00 seems appropriate for clarity of command but will require careful implementation to avoid the evolution of "stovepipes."
- Reevaluate current training practices with the assistance of outside organizations (military special operations forces (SOF)). Possibilities range from such simple actions as increasing the number of allotted training rounds to enhancing force-on-force testing methodology. (I am aware that many of the DoE security personnel have had earlier experience with the above organizations!)
- *Change the culture!* This can be facilitated by adopting the previously mentioned practices. It is emphasized that a primary benefit of the "Federalized Force" model is that it does provide a fresh start—a "clean sheet of paper."

CONCLUDING OBSERVATIONS

The President's Foreign Intelligence Advisory Board (PFIAB) included the following comment in its 1999 report regarding DoE: "A department saturated with cynicism, an

arrogant disregard for authority, and a staggering pattern of denial." While I observed nothing approaching the former two criticisms, the third does have resonance, at least with operations at Y-12. The pervasiveness of this sense of denial throughout DoE's physical security system was not determinable in the time available for this review. Nonetheless, there is ample reason to thoroughly reassess the activities at other sites in search of patterns of behavior that may also require corrective action.

No matter what management model is adopted, the same individuals are likely to populate it—with the exception of a few senior managers. Fortunately, the people we met during our assessment appeared to be individually highly capable and clearly dedicated, but often overwhelmed by a culture of accommodation and passiveness when in the presence of sub-par performance. Somehow, at least at Y-12, a culture of tolerance overcame a culture of performance. And while one could never, ever condone the actions of the trespassers on July 28, they inadvertently provided a much needed wakeup-call to those responsible for physical security at the nation's nuclear facilities. And while the Y-12 trespassers could not, in retrospect, pose a meaningful threat even given the extent of access they achieved, the magnitude of the failure of the security system was extraordinary. Strikingly, there have been incidents in earlier years at Savannah River and Rocky Flats that point to much the same cultural shortcomings as have been allowed to persist at Y-12. Change is needed...and needed quickly.

I would note that a great deal of additional information resides at CSIS, and I believe it would be a sound investment for it to be compiled and provided to the DoE.

Finally, I am honored that you requested that I participate in such an important undertaking and pleased that you encouraged me to be forthright in my assessment. I hope that my comments will be viewed as constructively offered and that they might assist you and the members of your team in addressing the challenges the nation confronts in securing nuclear assets.

Norman R. Augustine

Norman R. Augustine

This updated version (dated December 10th) of the original letter contains minor clarifying edits.

CARNEGIE
INSTITUTION FOR
SCIENCE

December 6, 2012

OFFICE OF THE PRESIDENT

Richard A. Meserve
rmeserve@carnegiescience.edu

SCIENTIFIC DEPARTMENTS

Embryology
BALTIMORE, MARYLAND

Geophysical Laboratory
WASHINGTON, DC

Global Ecology
STANFORD, CALIFORNIA

The Observatories
PASADENA, CALIFORNIA AND
LAS CAMPANAS, CHILE

Plant Biology
STANFORD, CALIFORNIA

Terrestrial Magnetism
WASHINGTON, DC

Carnegie Academy for
Science Education
WASHINGTON, DC

Carnegie Institution
of Washington

1530 P Street NW
Washington, DC 20005

202 387 6400 Office
202 387 8092 Fax

Secretary Steven Chu
U.S. Department of Energy
1000 Independence Ave SW
Washington, DC 20585

Dear Steve:

I am writing in response to your request for advice on the management of physical security at the facilities with Category I material under DOE control. You have explained that this request arose as a result of the event at the Y-12 Highly Enriched Uranium Materials Facility in July in which three people, including an elderly nun, were able to penetrate the security fences and to deface the exterior of the building before being apprehended. In addition to this troubling breach, the first responder's casual behavior upon encountering the intruders was completely inappropriate given the nature of the site.

The security challenge confronting the Department is a complicated one for a variety of reasons. The DOE approach to security has evolved since 9/11 from something that is akin to industrial security to a system involving an elite paramilitary force that can defend against a sophisticated terrorist attack. This has been a challenge both because of the need to enhance the capabilities of the protective forces and because the change has entailed significant expense to strengthen security structures and systems at facilities that were not initially designed with this type of security in mind. These changes had to be undertaken within budgetary limitations at a time when the Department needed to pursue many other important (and expensive) programs. The changing demands on the weapons complex over the years have added yet another layer of complexity. And any change in security had to be accomplished within a legal and administrative structure for the Department that is extraordinarily complicated.

The Department has not lacked for an abundance of thoughtful studies on the security issue over the years. Considerable change has been introduced as a result, but the Y-12 episode reveals that problems remain. Although my examination of the security issues confronting the Department has necessarily been limited, I am satisfied that the Y-12 episode has been taken very seriously and considerable effort has been made to ensure that security is strong throughout the complex. I have thus focused on your request to consider whether there are issues relating to the management structure for physical security. I know that you seek confidence that the security obligation will be fulfilled in an effective way for the long term.

You specifically asked whether the wholesale modification of the management structure for physical security is appropriate. As you know, the current system relies on contractors to provide security. (The details of this approach are discussed further below.) The obvious alternative would be to federalize the protective force (partially or completely) so that the security officers become DOE employees. Federalization could shorten chains of command between federal policymakers and the implementers of security, would encourage consistent application of policies and procedures across sites, would reflect the reality that security is a central federal function at these sites, and perhaps most importantly, would eliminate the potential for strikes by the protective force. Moreover, I understand that the unions at one time advocated such a change in order to deal with retirement and long-term disability concerns of the security officers.

An evaluation by DOE in 2009 concluded that the merits of federalization turned on three factors: implementation of elite force concepts in a cost-effective manner, determination of practical avenues to address retirement and disability concerns, and identification of methods to address potential protective force work stoppages. Memorandum to the Acting Deputy Secretary from T.P. D'Agostino and G.S. Podonsky (Jan. 13, 2009). The review found that the cost issue was the most important factor that should guide a decision and concluded that federalization would result in increased costs without commensurate benefits, particularly given the progress that had been made in implementing the elite force approach using contractors. The review also concluded that federalization did not offer a viable approach to address the union concerns because of the difficulties and complexities of a transition of guards from private-sector employment to federal employment. And, although it acknowledged that the most compelling reason to pursue federalization was to prevent work stoppages by unionized protective force members, it concluded that this risk could be managed by the execution of contingency protective force operations in such a situation, an approach that DOE has had to take in connection with a strike at Pantex. Although to my mind the issue is a close one, I have no informed basis to challenge this recent evaluation.

One additional factor in favor of federalization is that a dramatic change of this nature could facilitate the introduction of a new security culture. In a sense, such a step would serve to wipe the slate clean and demonstrate that very different performance is expected going forward. The Office of Secure Transport uses federal employees and has satisfactorily fulfilled its functions, which serves to show that federalization can work. But no doubt a wholesale change in management structure would be very expensive to accomplish. And, if the protective force were federal employees, the imposition of discipline would be more difficult and in the end federalization could reduce flexibility.

A variant is limited federalization. For example, one might federalize the armed component of the protective forces, while relying on a contractor for the remaining services. This presumably would reduce the cost of the transition

and would recognize the unique federal role of those who are authorized to use deadly force. Since federal employees cannot strike, this approach would facilitate the ability to respond to a work stoppage. But this approach would then complicate the chains of command within the protective forces. And it would make even more difficult the challenge of providing a career path for those in the armed component of the protective forces. (This issue is discussed below.)

I conclude that a decision to federalize all or a part of the protective force would be difficult, would be expensive to accomplish, and would create some new challenges. In the absence of compelling benefits, it is probably not warranted. But it is an approach that may be worthy of consideration if efforts to make the necessary changes cannot be accomplished by a less drastic approach.

A variant to the federalization of the protective force as DOE employees is to engage another federal agency, such as the Department of Defense or the Department of Homeland Security, to provide security. Engagement of another agency to provide security would serve to complicate chains of command and would likely create confusion as to who was in charge at the sites. The interfaces between the DOE and the management and operations ("M&O") contractors would become even more complicated and confusing. Even if DOE were to engage another agency to provide security, the Department would still be accountable for the security posture. And, although I have not pursued the point, I am doubtful that another agency would be willing take on the task. I conclude that such an approach is not suitable.

I thus conclude that it is reasonable to continue to rely on private contractors to provide security. I hasten to add, however, that there are opportunities to improve the management of security. Some of my suggestions follow:

1. Align authority and responsibility. At Y-12, there was a division of responsibility for physical protection between the contractor responsible for the protective officers and the M&O contractor responsible for the fences, various sensors and other equipment that are part of the physical protection system. The result was a fractured management structure. The interface between the contractors was clearly not functioning: their priorities were not aligned. Cameras in the affected area were out of service and had been for a considerable time and the system of detectors, which had recently been significantly upgraded, was plagued by frequent false alarms. This resulted in a situation in July in which the protective force did not appreciate that the alarms associated with the breach of the fences were "real" and the absence of functioning cameras did not enable the appropriate immediate surveillance of the situation. Although no doubt a system involving multiple contractors could be made to work, a simplified structure in which one contractor is

responsible for all elements of security would provide greater assurance that the security approach is integrated and that issues that otherwise would cross lines between contractors are addressed.

Although a compelling case can be made for assuring that all security functions are the responsibility of a single contractor, there is a subsidiary question whether security should be the subject of a separate contract from that with the M&O contractor. The advantage of separation is that the security responsibility could be allocated to an entity with strong skills in that one area, whereas the M&O contractor presumably must be selected based on a balancing of a variety of capabilities. But, again, separating the security function from the overall site responsibility will require a complicated interface between contractors, with opportunities for miscommunication and misalignment of priorities: security should be an integral part of site operations, not an add-on. Indeed, a single chain of command will be mandatory during a security event. As a result, the favored course, it seems to me, is to require the M&O contractor to fulfill the security function and to ensure, through proper controls, that it meets its responsibilities.

2. Improve federal oversight. It was apparent that the department's system of oversight did not detect and correct the security problems that the Y-12 incident revealed. The large number of false alarms was tolerated, raising questions about the acceptance testing, readiness, and maintenance of the ARGUS system. The cameras were not viewed as critical security equipment, with the result that a significant number were inappropriately allowed to remain out of service for an extended period. There were significant departures from expected procedures by the first responder, as well as significant communication deficiencies. The DOE oversight "system" was seemingly unaware of these problems and, in fact, the evaluations of the security at Y-12 had received consistently high marks in the period before the incident. The overall situation reveals significant failings in oversight by DOE. I appreciate that the approach to oversight does implicate broader issues within the Department as to the degree of freedom and flexibility that should be provided to its contractors.

   Part of the challenge in providing proper oversight may relate to the extraordinarily complicated administrative structure within DOE, with security responsibilities spread across several offices at headquarters and between headquarters and the DOE field offices. Indeed, we have had some difficulty in obtaining a clear organization chart that defines the structure for security oversight within DOE. I understand that issues associated with diffuse management are subject to study within the National Nuclear Security Administration ("NNSA") in an effort that is being led by Brigadier General Sandra Finan. A broader examination of DOE's internal management of security should be undertaken in order to

streamline and simplify the structure. The aim should be to establish clear authority and responsibility and to assure that the responsible staff has the right training and experience. Although I appreciate that different approaches to security may well be appropriate as a result of differing circumstances at the various DOE sites, I question whether different standards can be justified as a result of DOE's organizational structure. Efforts to achieve consistency and uniformity would be appropriate.

3. Enhancement of the Protective Force. Perhaps the most puzzling aspect of the Y-12 incident is the behavior of the first responder. He had evidently received the appropriate training, but decided to ignore it. He seems to have immediately concluded that the three intruders were not a threat and, as a result, he treated them as such. Although his assessment proved to be correct, attackers might seek cover for a serious assault by mimicking the appearances that evidently were so reassuring to the first responder. The episode reveals the importance of training and drills to reinforce appropriate actions by the protective force.

   There are challenges associated with the maintenance of an appropriately trained protective force. DOE has enhanced the capabilities of its protective forces significantly with the aim of a establishing an elite paramilitary capability that can respond to a very capable and sophisticated adversary. The physical qualifications and capabilities of many members of the force must be maintained at a high level, which creates a challenge in establishing a career trajectory for the protective officers. Having a force that maintains its "edge" is difficult, given that actual attacks have not occurred. Indeed, overcoming boredom among the members of the protective force is difficult. The commercial nuclear industry has confronted many of these same challenges and has sought to establish and maintain an esprit among the protective force. It encourages attentiveness by frequent force-on-force drills, regular transitions among posts, and allowing other activities, such as access to the web while on post, in appropriate circumstances. It has sought to respond to the demanding physical challenges that may become more difficult as the security officers age by enabling and encouraging them to migrate to other jobs at the site. In short, it has sought to establish and reinforce that the protective force is an important part of the team that operates the plant and that its members have career opportunities. Some of these lessons may be relevant to the DOE sites.

4. Security Culture. The commercial nuclear industry has learned that the essential ingredient for assuring safe operations is the establishment of a culture in which safety is the highest priority. Management has the obligation to establish such a culture by its words and deeds, including the allocation of resources. Each plant worker has an individual responsibility to assure that any safety issue that a worker observes is

addressed even it is not within the worker's responsibilities; if a supervisor fails to respond, the worker is obligated to raise the issue to a higher level and severe sanctions are imposed if any retaliation against such a worker occurs. Given the critical importance of security at the Category I sites, I believe that an analogous security culture needs to be established at the DOE sites. That is, everyone on the site should understand that security is his or her responsibility. Establishing such a culture will be difficult in a system in which individuals are otherwise encouraged to focus on individual responsibilities, but truly effective security requires such a change.

5. Balance. The Y-12 episode has appropriately caused a heightened awareness of the importance of physical security. This focus should not be allowed to unduly distort DOE's efforts. The aim should be to evaluate security using a systems approach that integrates physical, cyber, and personnel security in order to reduce aggregate vulnerabilities. Balance should be maintained.

* * *

In developing my thinking on the charge that you presented, I have had the benefit of interactions with Norm Augustine and Don Alston, as well as substantial assistance from the Center for Strategic and International Studies ("CSIS"). I was aided by extensive materials assembled by CSIS with DOE assistance concerning the various security reviews undertaken over the years, by site visits, by discussions with DOE and contractor staff, and by interviews with knowledgeable individuals. (Some of these interviews were undertaken by CSIS staff.) I very much appreciate this assistance. Nonetheless, this letter reflects my perspective. My comments should not be attributed to the various individuals who have helped to shape my judgments.

I hope this letter is helpful. Please feel free to contact me if you have any questions.

Best regards.

Very truly yours,

Richard A. Meserve

Mr. MURPHY. Thank you very much.

Mr. Trimble, you have a chance for an opening statement.

TESTIMONY OF DAVID C. TRIMBLE

Mr. TRIMBLE. Thank you, Chairman Murphy, Ranking Member DeGette, members of the subcommittee. My testimony today discusses DOE's and NNSA's management of the nuclear security enterprise, and will focus on security, safety, and project and contract management.

Multiple investigations into the security breach at Y–12 identified significant deficiencies in NNSA's security organization, oversight, and culture. In response to the Y–12 security incident and the findings of these reports, DOE and NNSA have taken a number of actions, including repairing security equipment, reassigning key security personnel, and firing the Y–12 protective force contractor. More recently, DOE and NNSA's leadership committed to additional actions, such as revamping the security oversight model. We have not evaluated these recent actions but will examine them as part of our ongoing review on security reform for this committee.

The key question underlying this work will be whether DOE's actions to address the security breakdowns at Y–12 will produce sustained improvements in security across the nuclear security enterprise.

DOE has a long history of security breakdowns and an equally long history of instituting responses and remedies to fix these problems. The recent testimony the leader of the NNSA security task force examining the Y–12 incident identified problems at NNSA's federal security organization, including poorly defined roles and responsibilities for its headquarters and field staff, inadequate oversight and assessments of secured activities, problems ensuring that security improvements are implemented, and failing to ensure adequate staffing. Notably, in 2003, we reported on these same problems, problems which have persisted or resurfaced, notwithstanding numerous DOE initiatives to fix or address them.

In examining the security incident at Y–12, it is also important to remember that NNSA's security problems have not been limited to Y–12. In March of 2009, we reported on numerous and wide-ranging security deficiencies at Livermore, particularly in the ability of Livermore's protective forces to ensure the protection of special nuclear material and the laboratory's protection control of classified material. We also identified Livermore's physical security systems, such as alarms and sensors, and its security assurance activities as areas needing improvement. Weaknesses in Livermore's contractor self-assessment program and the Livermore site office's oversight of the contractor contributed to these security deficiencies at the laboratory.

Los Alamos experienced a number of high profile security incidents in the '90s that were subject to numerous congressional hearings, including some held by this committee. Subsequently, security evaluations through 2007 identified other persistent systemic security problems, including weaknesses in controlling protecting classified resources, inadequate controls over special nuclear matter, inadequate self-assessment activities, and weaknesses in the process Los Alamos uses to ensure that corrects identified security defi-

ciencies. In October of 2009, we found weaknesses at Los Alamos in protecting the confidentiality, integrity, and availability of information stored on and transmitted over its classified computer network.

Regarding safety, in September of 2012, we testified before this subcommittee, noting that DOE's recent safety reforms may have actually weakened independent oversight. Notably, since this recent testimony, reports by DOE and the safety board have continued to identify safety concerns at Y–12, Pantex, and Los Alamos.

Regarding project management, DOE has made progress in managing the costs and scheduled non-major projects, those costing less than $750 million, and in recognition of this progress, GAO has narrowed the focus of our high risk designation to major contracts and projects. Major projects, however, continue to pose a challenge for DOE and NNSA. In December of 2012, we reported that the estimated cost to construct the waste treatment and immobilization plant in Hanford, Washington, had tripled to $12.3 billion since its inception in 2000, and the scheduled completion date had slipped nearly a decade to 2019. Moreover, we found that DOE had prematurely rewarded the contractor for resolving technical issues and completing work. We have reported on similar problems with the CMR facility at Los Alamos, the EPF project at Y–12, and the MOX project at Savannah River.

In conclusion, over a decade after NNSA was created to address security issues, the Y–12 security incident has raised concern that NNSA has still not embraced security as an essential element of its mission. The numerous actions that DOE and NNSA are taking to address its security problems will require effective implementation across the complex. Without this and strong and sustained leadership, these recent reforms, like past efforts, may not have a lasting impact on the security, performance, or culture of the agency.

Thank you. I would be pleased to answer any questions you may have.

[The prepared statement of Mr. Trimble follows:]

United States Government Accountability Office

GAO

Testimony

Before the Subcommittee on Oversight and Investigations, Committee on Energy and Commerce, House of Representatives

For Release on Delivery
Expected at 10 a.m. EDT
Wednesday, March 13, 2013

MODERNIZING THE NUCLEAR SECURITY ENTERPRISE

Observations on DOE's and NNSA's Efforts to Enhance Oversight of Security, Safety, and Project and Contract Management

Statement of David C. Trimble, Director
Natural Resources and Environment

GAO
Accountability * Integrity * Reliability

GAO-13-482T

GAO
Accountability * Integrity * Reliability

Highlights

Highlights of GAO-13-482T, a testimony before the Subcommittee on Oversight and Investigations, Committee on Energy and Commerce, House of Representatives.

March 2013

MODERNIZING THE NUCLEAR SECURITY ENTERPRISE

Observations on DOE's and NNSA's Efforts to Enhance Oversight of Security, Safety, and Project and Contract Management

Why GAO Did This Study

DOE and NNSA are responsible for managing nuclear weapon- and nonproliferation-related national security activities in national laboratories and other sites and facilities, collectively known as the nuclear security enterprise. Major portions of NNSA's mission are largely carried out by contractors at each site. GAO has designated contract management of major projects (i.e., those $750 million or more) at DOE and NNSA as a high risk area. Progress has been made, but GAO continues to identify security and safety problems at DOE and NNSA sites as well as project and contract management problems related to cost and schedule overruns on major projects.

This testimony addresses DOE's and NNSA's oversight of (1) security performance, (2) safety performance, and (3) project and contract management in the nuclear security enterprise. It is based on prior GAO reports issued from August 2000 to December 2012.

DOE and NNSA continue to act on the numerous recommendations GAO has made to improve management of the nuclear security enterprise. GAO will continue to monitor DOE's and NNSA's implementation of these recommendations.

View GAO-13-482T. For more information, contact David C. Trimble, (202) 512-3841 or trimbled@gao.gov

What GAO Found

The Department of Energy (DOE) and the National Nuclear Security Administration (NNSA), a separately organized agency within DOE, continue to face challenges in ensuring that oversight of security activities is effective. For example, in July 2012, after three trespassers gained access to the protected security area directly adjacent to one of the nation's most critically important nuclear weapon-related facilities, the Y-12 National Security Complex, DOE and NNSA took a number of immediate actions. These actions included repairing security equipment, reassigning key security personnel, and firing the Y-12 protective force contractor. As GAO and others have reported, DOE has a long history of security breakdowns and an equally long history of instituting remedies to fix these problems. For example, 10 years ago, GAO reported on inconsistencies among NNSA sites on how they assess contractors' security activities and, since that time, DOE has undertaken security initiatives to address these issues. GAO is currently evaluating these security reform initiatives.

DOE and NNSA continue to face challenges in ensuring that oversight of safety performance activities is effective. DOE and NNSA have experienced significant safety problems at their sites, and recent efforts to reform safety protocols and processes have not demonstrated sustained improvements. Long-standing DOE and NNSA management weaknesses have contributed to persistent safety problems at NNSA's national laboratories. For example, in October 2007, GAO reported that nearly 60 serious accidents or near misses had occurred at NNSA's national laboratories since 2000. DOE has undertaken a number of reforms to address persistent safety concerns. For example, in March 2010, the Deputy Secretary of Energy announced a reform effort to revise DOE's safety and security directives. However, GAO reported in September 2012 that DOE's safety reforms did not fully address continuing safety concerns that GAO and others identified in the areas of quality assurance, safety culture, and federal oversight and, in fact, may have actually weakened independent oversight.

DOE and NNSA have made progress but need to make further improvements to their contract and project management efforts. DOE has made progress in managing nonmajor projects—those costing less than $750 million—and in recognition of this progress, GAO narrowed the focus of its high-risk designation of DOE's Office of Environmental Management (EM) and NNSA to major contracts and projects. Specifically, as GAO noted in its December 2012 report on 71 DOE EM and NNSA nonmajor projects, GAO found the use of some sound management practices that were helping ensure successful project completion. However, major projects continue to pose a challenge for DOE and NNSA. For example, in December 2012, GAO reported that the estimated cost to construct the Waste Treatment and Immobilization Plant in Washington State had tripled to $12.3 billion since its inception in 2000, and the scheduled completion date had slipped by nearly a decade to 2019. Also, in March 2012, GAO reported that a now-deferred NNSA project to construct a new plutonium facility in Los Alamos, New Mexico, could cost as much as $5.8 billion, a nearly six-fold cost increase.

United States Government Accountability Office
Washington, DC 20548

Chairman Murphy, Ranking Member DeGette, and Members of the Subcommittee:

Thank you for the opportunity to discuss our work on the security, safety, and project management issues related to the nation's nuclear security enterprise. As you know, the National Nuclear Security Administration (NNSA), a separately organized agency within the Department of Energy (DOE), is responsible for managing nuclear weapon- and nonproliferation-related missions in research and development laboratories, production plants, and other facilities—known collectively as the nuclear security enterprise.[1] NNSA directs these national security missions, but work activities are largely carried out by management and operating (M&O) contractors at each site within the nuclear security enterprise. Working under M&O contracts, NNSA contractors apply their scientific, technical, and management expertise at NNSA's government-owned, contractor-operated sites.[2]

As we testified before this Subcommittee in September 2012,[3] questions have been raised about DOE's and NNSA's oversight of security, safety, and project and contract management for the nuclear security enterprise. For example, we first designated DOE's management of its contracts as an area at high risk of fraud, waste, abuse, and mismanagement in 1990 because of the department's record of inadequate management and oversight of its contractors. During the late 1990s, DOE experienced security problems at the nation's nuclear weapons laboratories and

[1]Specifically, NNSA manages three national nuclear weapon design laboratories—Lawrence Livermore National Laboratory in California, Los Alamos National Laboratory in New Mexico, and Sandia National Laboratories in New Mexico and California. It also manages four nuclear weapon production plants—the Pantex Plant in Texas, the Y-12 National Security Complex in Tennessee, the Kansas City Plant in Missouri, and the Tritium Extraction Facility at DOE's Savannah River Site in South Carolina. NNSA also manages the Nevada National Security Site, formerly known as the Nevada Test Site.

[2]M&O contracts are agreements under which the federal government contracts for the operation, maintenance, or support, on its behalf, of a government-owned or -controlled research, development, special production, or testing establishment wholly or principally devoted to one or more of the major programs of the contracting federal agency. Federal Acquisition Regulation, 48 C.F.R. § 17.601 (2012).

[3]GAO, *Modernizing the Nuclear Security Enterprise: Observations on the National Nuclear Security Administration's Oversight of Safety, Security, and Project Management*, GAO-12-912T (Washington, D.C.: Sept. 12, 2012).

significant cost overruns on major projects (i.e., $750 million or more). According to a June 1999 report by the President's Foreign Intelligence Advisory Board, DOE's management of the nuclear weapons laboratories, while representing "science at its best," also embodied "security at its worst" because of "organizational disarray, managerial neglect, and a culture of arrogance." The advisory board urged Congress to create a new organization that, whether established as an independent agency or a semiautonomous agency within DOE, would have a clear mission, streamlined bureaucracy, and drastically simplified lines of authority and accountability. Responding to the advisory board's recommendations, Congress created NNSA under Title 32 of the National Defense Authorization Act for Fiscal Year 2000—the NNSA Act.[4] The NNSA Act established NNSA as a "separately organized agency" within DOE. The act established the position of DOE Under Secretary for Nuclear Security, who was also designated as the Administrator of NNSA. The Secretary of Energy and the Deputy Secretary of Energy were allowed to establish policy for NNSA and to give direction to NNSA through the Administrator; however, other DOE employees were prohibited from directing the activities of individual NNSA employees. DOE directives remain the primary means to establish, communicate, and institutionalize policies, requirements, responsibilities, and procedures for multiple departmental elements, including NNSA, but the act gives the NNSA Administrator the authority to establish NNSA-specific policies, unless disapproved by the Secretary of Energy. NNSA does this through the issuance of Policy Letters.[5]

NNSA's creation, however, has not yet had the desired effect of fully resolving long-standing management problems. For example, NNSA and DOE's Office of Environmental Management (EM) remain on our high-risk list.[6] Furthermore, we have frequently reported on security incidents and safety issues that have contributed to the temporary shutdown of facilities, such as at Los Alamos and Lawrence Livermore National

[4]Pub. L. No. 106-65, 113 Stat. 512, 953 (1999).

[5]NNSA, *Policy Letters: NNSA Policies, Supplemental Directives, and Business Operating Procedures*, NA SD 251.1 (Washington, D.C.: July 5, 2011).

[6]GAO, *High-Risk Series: An Update*, GAO-13-283 (Washington, D.C.: Feb. 2013). We have shifted our focus concerning the high-risk area to major DOE-EM and NNSA major projects (i.e., those $750 million or more).

Laboratories in 2004 and 2005,[7] as well as the safety and security initiatives that contractors at these laboratories put in place to help ensure improvement. More recently, at the Y-12 National Security Complex, in July 2012, three trespassers gained access to the protected security area directly adjacent to one of the nation's most critically important nuclear weapon-related facilities without being interrupted by the security measures in place. According to DOE's Inspector General, this security incident was unprecedented and represented multiple system failures including failures to maintain critical security equipment, respond properly to alarms, and understand security protocols.[8] Furthermore, the Inspector General found that contractor governance and federal oversight did not identify and correct early indications of these multiple system breakdowns.

DOE's management approach to security over the years has shifted in part due to concerns raised by some national laboratory, DOE, and NNSA officials. These officials believed that DOE's and NNSA's oversight of the laboratories' activities had become excessive and that the safety and security requirements for the laboratories are overly prescriptive and burdensome, which had resulted in a negative effect on the quality of science performed at these laboratories. Partly in response to these concerns, DOE and NNSA embarked on reforms in 2010 and 2011 that sought to streamline requirements and institute what has been called by the National Research Council, the DOE Inspector General, the DOE Office of Health and Safety Performance, and the Defense Nuclear Facilities Safety Board (Safety Board) a "hands-off, eyes-on" role for federal oversight. This approach placed more reliance on contractors' self-oversight through its contractor assurance systems to ensure such things as effective safety and security performance.[9] Building on this theme, in February 2012, the National Research Council found that

[7]For additional information on the 2004 temporary shutdown of facilities at Los Alamos, see GAO, *Stand-Down of Los Alamos National Laboratory: Total Costs Uncertain; Almost All Mission-Critical Programs Were Affected but Have Recovered*, GAO-06-83 (Washington, D.C.: Nov. 18, 2005).

[8]DOE Office of Inspector General, *Inquiry into the Security Breach at the National Nuclear Security Administration's Y-12 National Security Complex*, DOE/IG-0868 (August 2012).

[9]These systems include management controls that help ensure the department's program missions and activities are executed in an effective, efficient, and safe manner. We are currently evaluating the implementation of contractor assurance systems at NNSA sites and NNSA's oversight of these systems.

"safety and security systems at the [NNSA] Laboratories have been strengthened to the point where they no longer need special attention."[10]

In this context, there have been calls to enhance NNSA's ability to operate independently of DOE. For example, the Defense Science Board proposed in 2006 that a completely independent nuclear weapons agency be created.[11] In January 2007, we reported that former senior DOE and NNSA officials with whom we spoke generally did not favor removing NNSA from DOE.[12] Furthermore, in a June 2012 report, we concluded that such a drastic change was unnecessary to produce an effective organization,[13] and we generally hold this view today. However, in the wake of the Y-12 security incident and persistent problems with major projects, there have been renewed calls to reexamine NNSA's organization. Most recently, the Fiscal Year 2013 National Defense Authorization Act created the Congressional Advisory Panel on the Governance of the Nuclear Security Enterprise to examine options and make recommendations for revising the governance structure, mission, and management of the nuclear security enterprise.

My testimony today discusses DOE's and NNSA's management of the nuclear security enterprise. It focuses on our reports issued from August 2000 to December 2012 on oversight of (1) security performance, (2) safety performance, and (3) project and contract management in the nuclear security enterprise. Detailed information about the scope and methodology can be found in our previously issued reports. We conducted the performance audit work that supports this statement in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain

[10]National Research Council, *Managing for High-Quality Science and Engineering at the NNSA National Security Laboratories*, (Washington, D.C.: Feb. 15, 2012).

[11]The Defense Science Board provides the Department of Defense with independent advice and recommendations on matters relating to the department's scientific and technical enterprise. See Defense Science Board Task Force, *Nuclear Capabilities* (Washington, D.C.: Dec. 2006).

[12]GAO, *National Nuclear Security Administration: Additional Actions Needed to Improve Management of the Nation's Nuclear Programs*, GAO-07-36 (Washington, D.C.: Jan.19, 2007).

[13]GAO, *Modernizing the Nuclear Security Enterprise: Observations on the Organization and Management of the National Nuclear Security Administration*, GAO-12-867T (Washington, D.C.: June 27, 2012).

sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

DOE is responsible for a diverse set of missions, including nuclear security, energy research, and environmental cleanup. These missions are managed by organizations within DOE and largely carried out by M&O contractors at various DOE sites. According to federal budget data, NNSA is one of the largest organizations in DOE, overseeing nuclear weapons, nuclear nonproliferation, and naval reactors missions at its sites. With an $11 billion budget in fiscal year 2012—nearly 40 percent of DOE's total budget—NNSA is responsible for providing the United States with safe, secure, and reliable nuclear weapons in the absence of underground nuclear testing and maintaining core competencies in nuclear weapons science, technology, and engineering. Ensuring a safe and reliable nuclear weapons stockpile is an extraordinarily complicated task and requires state-of-the-art experimental and computing facilities, as well as the skills of top scientists in the field. To its credit, NNSA consistently accomplishes this task, as evidenced by the successful assessment of the safety, reliability, and performance of each weapon type in the nuclear stockpile since its creation. To support these capabilities into the future, in 2011, the administration announced plans to request $88 billion from Congress over the next decade to operate and modernize the nuclear security enterprise.

As discussed earlier, work activities to support NNSA's national security missions are largely carried out by M&O contractors. This arrangement has historical roots. Since the Manhattan Project produced the first atomic bomb during World War II, NNSA, DOE, and predecessor agencies have depended on the expertise of private firms, universities, and others to carry out research and development work and efficiently operate the facilities necessary for the nation's nuclear defense. Currently, DOE spends 90 percent of its annual budget on M&O contracts, making it the largest non-Department of Defense contracting agency in the government.

DOE generally regulates the safety of its own nuclear facilities and operations at its sites. In contrast, the Nuclear Regulatory Commission

(NRC) generally regulates commercial nuclear facilities, and the Occupational Safety and Health Administration (OSHA) generally regulates worker safety at commercial industrial facilities.[14] However, because of the dangerous nature of work conducted at many sites within the nuclear security enterprise—handling nuclear material such as plutonium, manufacturing high explosives, and various industrial operations that use hazardous chemicals—oversight of the nuclear security enterprise is multifaceted. First, DOE policy states that its M&O contractors are expected to develop and implement an assurance system, or system of management controls, that helps ensure the department's program missions and activities are executed in an effective, efficient, and safe manner.[15] Through these assurance systems, contractors are required to perform self-assessments as well as identify and correct negative performance trends. Second, NNSA site offices, which are collocated with NNSA sites, oversee the performance of M&O contractors. Site office oversight includes communicating performance expectations to the contractor, reviewing the contractor's assurance system, and conducting contractor performance evaluations. Third, DOE's Office of Health, Safety, and Security—especially its Office of Independent Oversight—conducts periodic appraisals to determine if NNSA officials and contractors are complying with safety and security requirements.[16] Fourth, NNSA receives safety assessments and recommendations from other organizations, most prominently the Safety Board—an independent executive branch agency created by Congress to assess safety conditions and operations at DOE's defense nuclear facilities.[17] To address public health and safety issues, the Safety Board is authorized to make recommendations to the Secretary of Energy, who

[14]DOE regulates the safety of most of its own sites with nuclear operations; NRC regulates several DOE nuclear facilities, and OSHA regulates occupational safety at DOE sites that have no nuclear function.

[15]DOE, *Department of Energy Oversight Policy*, DOE P 226.1B (Washington, D.C.: Apr. 25, 2011). Contractor assurance systems are to cover the following operational aspects: (1) environment, safety, and health; (2) safeguards and security; (3) emergency management; and (4) cyber security.

[16]DOE reorganized offices within its Office of Health, Safety, and Security. The Office of Independent Oversight merged with the Office of Enforcement and was renamed the Office of Enforcement and Oversight. For the purposes of this report, we refer to it as the Office of Independent Oversight.

[17]The Safety Board provides oversight for all NNSA sites except the Kansas City Plant, which manufactures non-nuclear components.

may then accept or reject, in whole or in part, the recommendations. If the Secretary of Energy accepts the recommendations, the Secretary must prepare an implementation plan.

DOE and some of its contractors have viewed this multifaceted oversight to be overly burdensome. To address this issue, in March 2010 the Deputy Secretary of Energy announced a reform effort to revise DOE's safety and security directives and modify the department's oversight approach to "provide contractors with the flexibility to tailor and implement safety and security programs without excessive federal oversight or overly prescriptive departmental requirements." In the memorandum announcing this effort, the Deputy Secretary noted that burdensome safety requirements were affecting the productivity of work at DOE's sites and that reducing this burden on contractors would lead to measurable productivity improvement. The Deputy Secretary noted that DOE's Office of Health, Safety and Security in 2009 had begun reforming its approach to enforcement and oversight. Similar to, but independent of DOE's safety and security reform effort, in February 2011, NNSA initiated its "governance transformation" project, which involved revising the agency's business model to, among other things, place more reliance on contractors' self-oversight through its contractor assurance system to ensure such things as effective safety and security performance. NNSA's non-nuclear Kansas City Plant completed implementation of this new business model, and other NNSA sites—such as the Nevada National Security Site and the Y-12 National Security Complex—were in the process of implementing it, too, when the Y-12 security incident occurred.

DOE's and NNSA's Oversight of Security Performance Continues to Face Challenges

In response to the Y-12 security breach, multiple investigations and reviews of the incident were performed by NNSA, the DOE Office of Inspector General, and the DOE Office of Independent Oversight. These reviews identified numerous problems with NNSA's and its contractors' performance, including: physical security systems, such as alarms; protective force (i.e., NNSA's heavily armed, contractor guard forces) training and response; failures to correct numerous known problems; and weaknesses in contract and resource management. In addition, at the request of the Secretary of Energy, an independent panel, composed of three former executives from Federal agencies and the private sector, and a NNSA Security Task Force found broader and systemic security issues across the nuclear security enterprise. The Secretary's panel in December 2012 analyzed various models for providing security at DOE and NNSA sites but generally found that improvements to the security culture, management, and oversight were necessary, in addition to having

an effective organizational structure. In addition, the leader of the NNSA Security Task Force testified before the House Armed Services Committee in February 2013 about significant deficiencies in NNSA's entire security organization, oversight, and culture.

In response to the Y-12 security incident and these findings, DOE and NNSA took a number of immediate actions, including repairing security equipment, reassigning key security personnel, and firing the Y-12 protective force contractor. In February 2013, the Acting NNSA Administrator committed to implementing a three-tiered oversight process involving contractor self-assessment, NNSA evaluation of site performance, and independent oversight by DOE's Office of Independent Oversight. The Acting Administrator testified before the House Armed Services Committee that she believed that such actions will help instill a culture that embraces security as an essential element of NNSA's missions.

In assessing DOE's actions to address the security breakdowns at Y-12, a central question will be whether these latest actions taken will produce sustained improvements in security at Y-12 and across the nuclear security enterprise. As we and others have reported, DOE has a long history of security breakdowns and an equally long history of instituting responses and remedies to "fix" these problems. For example, in examining the Y-12 security incident, NNSA's former Acting Chief of Defense Nuclear Security and the leader of the NNSA's Security Task Force testified in February 2013 about problems with NNSA's federal security organization including poorly defined roles and responsibilities for its headquarters and field security organizations, inadequate oversight and assessments of site security activities, and issues with overseeing contractor actions and implementing improvements. As noted in table 1, 10 years ago we reported on very similar problems, and since that time DOE has undertaken numerous security initiatives to address them. We have not evaluated these recent initiatives but we have ongoing work to evaluate them as part of our review on security reform for the Subcommittee, which we will complete later this year.

Table 1: Comparison of GAO 2003 Findings Regarding NNSA's Federal Security Organization with NNSA Security Task Force's February 2013 Findings

	GAO May 2003 Findings	NNSA Security Task Force February 2013 Findings
Defining clear roles and responsibilities	NNSA has not fully defined clear roles and responsibilities for its headquarters and site operations.	NNSA security line management authority is ill-defined. There are overlapping lines of authority and a mixing of staff and line functions.
Assessing sites' security activities	There are inconsistencies among NNSA sites on how they assess contractors' security activities. Consequently, NNSA cannot be assured that all facilities are subject to comprehensive annual assessments as required by DOE policy.	NNSA does not have an adequate security performance assessment process or capability. NNSA has come to rely overwhelmingly on federal staff reviewing contractor-provided data, rather than effectively assessing performance itself.
Overseeing contractors' actions and implementing long-term improvements	NNSA contractors do not consistently conduct required analyses in preparing security corrective program action plans. Security performance at sites may not be maximized because corrective security program actions are developed without fully considering root causes, risks posed, or costs and benefits of taking corrective action.	NNSA has attempted to correct some identified issues over the years, but it has not adequately emphasized security mission performance. Recent DOE and NNSA reforms have deemphasized performance verification by federal staff, resulting in a weakened federal security assessment program.
Allocating staff	NNSA has shortfalls at its site offices in number and expertise of staff, which could make it more difficult for site offices to effectively oversee security activities.	The NNSA federal security function is not properly organized or staffed.

Sources: GAO, *Nuclear Security: NNSA Needs to Better Manage Its Safeguards and Security Program*, GAO-03-471 (Washington, D.C.: May 30, 2003); and Hearing on Nuclear Security: Actions, Accountability, and Reform, Before the Subcommittee on Strategic Forces, House Armed Services Committee, 113th Cong. (Feb. 28, 2013) (Statement of Brigadier General Sandra E. Finan, Commander, Air Force Nuclear Weapons Center. Testimony based on Previous Position as Acting Chief of Defense Nuclear Security, NNSA).

It is also important to note that NNSA's long-standing security problems are not limited to Y-12. DOE's and NNSA's work with nuclear materials such as plutonium and highly enriched uranium, nuclear weapons and their components, and large amounts of classified data require extremely high security, however, as we and DOE have reported, NNSA and DOE have a long history of poor security performance across the nuclear security enterprise, most notably at Los Alamos and Livermore national laboratories, as well as ongoing struggles to sustain security improvements, including information security.[18]

[18] We note that over the past decade, the DOE Inspector General and Office of Independent Oversight periodically identified serious security issues at almost all of NNSA's sites, including Sandia National Laboratories; the Nevada National Security Site, Pantex, and prior to the July 2012 security incident, the Y-12 National Security Complex.

Los Alamos National Laboratory

As we noted in our September 2012 testimony,[19] Los Alamos National Laboratory (Los Alamos) experienced a number of high-profile security incidents in the previous decade that were subject to congressional hearings, including some held by this Subcommittee. Many of these incidents focused on Los Alamos's inability to account for and control its classified resources. These incidents include the transfer or removal of classified information from authorized work areas or the laboratory itself, the temporary loss of two hard drives containing nuclear weapon design information, and difficulties in accounting for classified removable electronic media. In addition to these well-publicized incidents, security evaluations through 2007 identified other persistent, systemic security problems at Los Alamos. These problems included weaknesses in controlling and protecting classified resources, inadequate controls over special nuclear material, inadequate self-assessment activities, and weaknesses in the process that Los Alamos uses to ensure it corrects identified security deficiencies. Partly as a result of these findings, as we reported in 2008,[20] Los Alamos underwent a 10 month shut-down of operations in 2004 and experienced a change in contractors in 2005. Moreover, the Secretary of Energy issued a compliance order in 2007 requiring Los Alamos to implement specific corrective actions to, among other things, address long-standing deficiencies in its classified information programs. We reported in January 2008 and testified before this Subcommittee in September 2008 that Los Alamos had experienced a period of improved security performance but that it was too early to determine whether NNSA and Los Alamos could sustain this level of improvement.[21]

Lawrence Livermore National Laboratory

In March 2009, we reported on numerous and wide-ranging security deficiencies at Lawrence Livermore National Laboratory (Livermore), particularly in the ability of Livermore's protective forces to ensure the

[19]GAO-12-912T.

[20]GAO, *Los Alamos National Laboratory: Long-Term Strategies Needed to Improve Security and Management Oversight*, GAO-08-694 (Washington, D.C.: June 13, 2008).

[21] GAO, *Los Alamos National Laboratory: Information on Security of Classified Data, Nuclear Material Controls, Nuclear and Worker Safety, and Project Management Weaknesses*, GAO-08-173R (Washington D.C.: Jan. 10, 2008), and GAO, *Nuclear Security: Los Alamos National Laboratory Faces Challenges in Sustaining Physical and Cyber Security Improvements*, GAO-08-1180T (Washington, D.C.: Sep. 25, 2008).

protection of special nuclear material and the laboratory's protection and control of classified matter.[22] We also identified Livermore's physical security systems, such as alarms and sensors, and its security program planning and assurance activities, as areas needing improvement. Weaknesses in Livermore's contractor self-assessment program and the Livermore Site Office's oversight of the contractor contributed to these security deficiencies at the laboratory. According to one DOE Office of Independent Oversight official, both programs were "broken" and missed even the "low-hanging fruit." The laboratory took corrective action to address these deficiencies, but we noted that better oversight was needed to ensure that security improvements were fully implemented and sustained. In September 2012, NNSA and Livermore completed efforts to move the site's most sensitive nuclear material to other sites, thereby easing the site's security requirements.

Information Security

We also have reported extensively on NNSA's challenges in maintaining effective and secure information security systems, particularly at Los Alamos. For example, in June 2008, we reported that significant information security problems at Los Alamos had received insufficient attention.[23] The laboratory had over two dozen initiatives under way that were principally aimed at reducing, consolidating, and better protecting classified resources. However, the laboratory had not implemented complete security solutions to address either the problems of classified parts storage in unapproved storage containers or weaknesses in its process for ensuring that actions taken to correct security deficiencies were completed. In addition, in October 2009 we reported that Los Alamos needed to better protect its classified network.[24] Specifically, we found significant weaknesses remained in protecting the confidentiality, integrity, and availability of information stored on and transmitted over its classified computer network. Moreover, we found the laboratory's

[22]GAO, *Nuclear Security: Better Oversight Needed to Ensure That Security Improvements at Lawrence Livermore National Laboratory Are Fully Implemented and Sustained*, GAO-09-321 (Washington, D.C.: Mar. 16, 2009).

[23]GAO, *Los Alamos National Laboratory: Long-Term Strategies Needed to Improve Security and Management Oversight*, GAO-08-694 (Washington, D.C.: June 13, 2008).

[24]GAO, *Information Security: Actions Needed to Better Manage, Protect, and Sustain Improvements to Los Alamos National Laboratory's Classified Computer Network*, GAO-10-28 (Washington, D.C.: Oct. 14, 2009).

decentralized approach to information security program management has led to inconsistent implementation of policy.

DOE and NNSA's Oversight of Safety Performance Continues to Face Challenges

DOE and NNSA have experienced significant safety problems at their sites, and recent efforts to reform safety protocols and processes have not demonstrated sustained improvements. As we testified in September 2012 before this Subcommittee,[25] long-standing DOE and NNSA management weaknesses have contributed to persistent safety problems at NNSA's national laboratories. For example, in October 2007, we reported that nearly 60 serious accidents or near misses had occurred at NNSA's national laboratories since 2000.[26] These accidents included worker exposure to radiation, inhalation of toxic vapors, and electrical shocks. Although no one was killed, many of these accidents caused serious harm to workers or damage to facilities. As we also reported, at Los Alamos in July 2004, an undergraduate student who was not wearing required eye protection was partially blinded in a laser accident. Our review of nearly 100 safety studies—including accident investigations and independent assessments by the Safety Board and others issued since 2000—found that the contributing factors to these safety problems generally fell into three key categories: (1) relatively lax laboratory attitudes toward safety procedures, (2) laboratory inadequacies in identifying and addressing safety problems with appropriate corrective actions, and (3) inadequate oversight by NNSA site offices.[27] DOE's Office of Inspector General has also raised concerns about safety oversight by NNSA's site offices. Specifically, the Inspector General reported in June 2011 that NNSA's Livermore Site Office was not sufficiently overseeing its contractor to ensure that corrective actions were fully and effectively implemented for a program designed to limit worker exposure to beryllium, a hazardous metal essential for nuclear operations.[28]

[25]GAO-12-912T.

[26]GAO, *Nuclear and Worker Safety: Actions Needed to Determine the Effectiveness of Safety Improvement Efforts at NNSA's Weapons Laboratories*, GAO-08-73 (Washington, D.C.: Oct. 31, 2007).

[27]GAO-08-73.

[28]DOE Office of Inspector General, *Implementation of Beryllium Controls at Lawrence Livermore National Laboratory*, DOE/IG-0851 (Washington, D.C.: June 17, 2011).

DOE has undertaken a number of reforms to address persistent safety concerns. In March 2010, the Deputy Secretary of Energy announced a reform effort to revise DOE's safety and security directives. The reform effort was aimed at modifying the department's oversight approach to "provide contractors with the flexibility to tailor and implement safety and security programs without excessive federal oversight or overly prescriptive departmental requirements." As we reported to this Subcommittee in April 2012,[29] this reform effort reduced the number of safety related directives from 80 to 42 by eliminating or combining requirements the department determined were unclear, duplicative, or too prescriptive and by encouraging the use of industry standards. However, as we noted in September 2012 before this Subcommittee, DOE's safety reforms did not fully address safety concerns that we, as well as others, have identified in the areas of quality assurance, safety culture, and federal oversight and, in fact, these reforms may have actually weakened independent oversight. We stated, for example, that while DOE policy notes that independent oversight is integral to help ensure the effectiveness of safety performance, DOE's Office of Independent Oversight staff must now coordinate their assessment activities with NNSA site office management to maximize the use of resources. This arrangement raised our concern about whether Office of Independent Oversight staff would be sufficiently independent from site office management. In our April 2012 report, we recommended, among other things, that DOE develop a detailed reform plan and clearly define the oversight roles and responsibilities of DOE's Office of Independent Oversight staff to ensure that their work is sufficiently independent from the activities of DOE site office and contractor staff. DOE has taken steps to respond to these recommendations, including developing a plan aimed at improving safety management and drafting a memo from the Secretary of Energy reconfirming the department's commitment to independent oversight of safety and security.

However, since our September 2012 testimony,[30] concerns continue to be raised about safety performance and oversight at several NNSA sites, which indicate DOE's safety reforms have not brought about a sustained change in safety practices. The following are examples:

[29]GAO, *Nuclear Safety: DOE Needs to Determine the Costs and Benefits of Its Safety Reform Effort*, GAO-12-347 (Washington, D.C.: Apr. 20, 2012).

[30]GAO-12-912T.

- A November 2012 report by DOE's Office of Independent Oversight raised concerns about safety culture issues at NNSA's Pantex Plant. Among the concerns were reluctance by workers to raise safety problems for fear of retaliation and a perception that cost took priority over safety.
- At an October 2012 public hearing in Knoxville, Tennessee, the Safety Board noted that safety controls to prevent or mitigate consequences from accidents had not been fully incorporated into the design of a new uranium processing facility at Y-12. The Safety Board noted the facility's safety basis—a technical analysis that identifies potential accidents and hazards associated with a facility's operations and outlines controls to mitigate or prevent their impact on workers and the public—did not adequately address controls to protect workers or the public in the case of an earthquake or small fires, and did not adequately calculate reasonably conservative radiation exposure consequences that could lead to putting greater safety into the facility's design. The Safety Board further noted that these deficiencies raise the potential for significant impacts on public and worker safety.
- A January 2013 Office of Independent Oversight report reviewing the Los Alamos Site Office assessment of the contractor corrective action system found that the contractor had not implemented effective corrective actions for identified safety system problems. This report noted that the site office concluded that more than half of the 62 safety system items needing corrective action had been closed without adequate action or sufficient documentation. Moreover, in October 2012, NNSA issued a Preliminary Notice of Violation to a Los Alamos contractor for repeated electrical safety problems. NNSA's notice stated that insufficient oversight of subcontractor work by the contractor safety staff was among the contributing factors. NNSA fined the contractor $262,500.

DOE and NNSA Have Made Progress but Further Improvements Needed on Project and Contract Management

A basic tenet of effective management is the ability to complete projects on time and within budget. DOE has taken a number of actions to improve management of projects, including those overseen by NNSA. For example, DOE has updated project and contract management policies and guidance in an effort to improve the reliability of project cost estimates, better assess project risks, and better ensure project reviews that are timely and useful and identify problems early. In addition, in December 2010, the Deputy Secretary of Energy convened a DOE Contract and Project Management Summit to discuss strategies for additional improvement in contract and project management. The participants identified barriers to improved performance and reported in

April 2012 on the status of initiatives to address these barriers. DOE has continued to release guides for implementing its revised order for Program and Project Management for the Acquisition of Capital Assets (DOE O 413.3B), such as for cost estimating, using earned value management, and forming project teams. Further, DOE has taken steps to enhance project management and oversight by requiring peer reviews and independent cost estimates for projects with values of more than $100 million and by improving the accuracy and consistency of data in its central repository for project data.

DOE has made progress in managing nonmajor projects—those costing less than $750—million and in recognition of this progress, we narrowed the focus of our high-risk designation to major contracts and projects. Specifically, as we noted in our October 2012 report on DOE's EM cleanup projects funded by the American Recovery and Reinvestment Act, at the time of our analysis, 78 of 112 projects had been completed.[31] Of those completed projects, 92 percent met the performance standard of completing project work scope without exceeding the cost target by more than 10 percent, according to EM data. However, we made four recommendations to DOE in this report aimed at improving how EM manages and documents projects, particularly with respect to establishing key performance parameters such as project scope targets and baselines for cost and schedule. DOE concurred with all of our recommendations, recognizing that improvements could be made and that lessons learned from these projects can be applied to EM's broader portfolio of projects and activities. In addition, in December 2012, we reported that EM and NNSA were making some progress in managing the 71 nonmajor construction and cleanup projects that we reviewed and are expected to cost an estimated $10.1 billion in total.[32] For example, we identified some NNSA and EM nonmajor projects that used sound project management practices, such as the application of effective acquisition strategies, to help ensure the successful completion of these projects. We also recommended that NNSA and EM clearly define, document, and track the scope, cost, and completion date targets for each of their nonmajor

[31]GAO, *Recovery Act: Most DOE Projects Are Complete, but Project Management Guidance Could Be Strengthened*, GAO-13-23 (Washington D.C.: Oct. 15, 2012).

[32]GAO, *Department of Energy: Better Information Needed to Determine If Nonmajor Projects Meet Performance Targets*, GAO-13-129 (Washington, D.C.: Dec. 19, 2012).

projects and that EM clearly identify critical occupations and skills in its workforce plans. NNSA and EM agreed with these recommendations.

Notwithstanding these positive developments for nonmajor projects, major projects (i.e., those $750 million or more) continue to pose a challenge for DOE and NNSA. Since 1990 when we placed contract and project management on the high-risk list, we have reported on problems that principally involve ineffective oversight and poor management of contractors. Our recent work, as well as reporting by DOE, indicates that these problems continue. Examples are as follows:

- In December 2012, we reported that the estimated cost to construct the Waste Treatment and Immobilization Plant in Washington State had almost tripled to $12.3 billion since the project's inception in 2000, and the scheduled completion date had slipped by nearly a decade to 2019.[33] Moreover, we found that DOE's incentives and management controls were inadequate for ensuring effective project management and we also found instances where DOE prematurely rewarded the contractor for resolving technical issues and completing work.
- In March 2012, we reported that NNSA's project to construct a new plutonium facility, the Chemistry and Metallurgy Research Replacement Nuclear Facility, at Los Alamos could cost as much as $5.8 billion, a nearly six-fold increase from its original estimate.[34] While the facility may be large enough to support nuclear weapon stockpile requirements, our March 2012 report found that it is unclear if the facility will be large enough to accommodate DOE's non-weapon activities that involve plutonium—such as nonproliferation, nuclear forensics, and nuclear counterterrorism programs—because the department has not comprehensively studied its long-term research and storage needs.
- In November 2010, we reported that NNSA's plans to construct a modern Uranium Processing Facility at its Y-12 National Security Complex in Oak Ridge, Tennessee, had experienced significant cost

[33]GAO, *Hanford Waste Treatment Plant: DOE Needs to Take Action to Resolve Technical and Management Challenges*, GAO-13-38 (Washington, D.C.: Dec. 19, 2012).

[34]GAO, *Modernizing the Nuclear Security Enterprise: New Plutonium Research Facility at Los Alamos May Not Meet All Mission Needs*, GAO-12-337 (Washington, D.C.: Mar. 26, 2012).

increases.[35] More recently, in September 2011, NNSA estimated that the facility would cost from $4.2 billion to $6.5 billion to construct—a nearly seven-fold cost increase from the original estimate.

- In April 2010, we reported that weak management by DOE and NNSA had allowed the cost, schedule, and scope of ignition-related activities at the National Ignition Facility to increase substantially.[36] We reported that, since 2005, ignition-related costs have increased by around 25 percent—from $1.6 billion in 2005 to over $2 billion in 2010—and that the planned completion date for these activities had slipped from the end of fiscal year 2011 to the end of fiscal year 2012 or beyond. Ten years earlier, in August 2000, we had reported that poor management and oversight of the National Ignition Facility construction project at Lawrence Livermore National Laboratory had increased the facility's cost by $1 billion and delayed its scheduled completion date by 6 years.[37]
- In March 2010, we reported that NNSA's Mixed-Oxide Fuel Fabrication Facility currently being constructed at DOE's Savannah River Site in South Carolina had experienced delays, but project officials said that they expected to recover from these delays by the end of 2010 and planned for the start of operations on schedule in 2016. In addition, after spending about $730 million on design, NNSA has cancelled the pit disassembly and conversion facility and is now planning to use existing facilities at DOE's Savannah River and Los Alamos sites and will add equipment to the mixed oxide facility. NNSA is working on a cost and schedule estimate for the use of these existing facilities and for adding the additional equipment.

We have also issued several reports on the technical issues, cost increases, and schedule delays associated with NNSA's efforts to extend, through refurbishment, the operational lives of nuclear weapons in the

[35]GAO, *Nuclear Weapons: National Nuclear Security Administration's Plans for Its Uranium Processing Facility Should Better Reflect Funding Estimates and Technology Readiness*, GAO-11-103 (Washington, D.C.: Nov. 19, 2010).

[36]Ignition-related activities consist of the efforts separate from the facility's construction that have been undertaken to prepare for the first attempt at ignition—the extremely intense pressures and temperatures that simulate on a small scale the thermonuclear conditions created in nuclear explosions. See GAO, *Nuclear Weapons: Actions Needed to Address Scientific and Technical Challenges and Management Weaknesses at the National Ignition Facility*, GAO-10-488 (Washington, D.C.: Apr. 8, 2010).

[37]GAO, *National Ignition Facility: Management and Oversight Failures Caused Major Cost Overruns and Schedule Delays*, GAO/RCED-00-271 (Washington, D.C.: Aug. 8, 2000).

stockpile. For example, in March 2009, we reported that NNSA and the Department of Defense had not effectively managed cost, schedule, and technical risks for the B61 nuclear bomb and the W76 nuclear warhead refurbishments.[38] For the B61 life extension program, NNSA was only able to stay on schedule by significantly reducing the number of weapons undergoing refurbishment and abandoning some refurbishment objectives. Earlier, in December 2000, we similarly had reported that refurbishment of the W87 strategic warhead had experienced significant design and production problems that increased its refurbishment costs by over $300 million and caused schedule delays of about 2 years.[39]

In conclusion, the actions that DOE and NNSA have taken to address weaknesses in oversight of security, safety, and contract and project management are very important, but problems persist. While we have noted progress in the area of project management, we also observe that NNSA and DOE EM have not begun a new major project since taking these actions. The Y-12 security incident was an unprecedented event for the nuclear security enterprise and perhaps indicates that NNSA's organizational culture, over a decade after the agency was created to address security issues, still has not embraced security as an essential element of its missions. In terms of safety, DOE has recently taken the initiative to examine the safety culture at its sites. We believe, as do other organizations, including the DOE Inspector General and Safety Board, that a "hands off, eyes on" oversight approach for security, safety and contract and project management is insufficient and unwarranted until the department can demonstrate sustained improvement in all three areas. We will continue to monitor DOE's and NNSA's implementation of actions to resolve its safety, security, and contract and project management difficulties and to assess the impact of these actions.

Chairman Murphy, Ranking Member DeGette, and Members of the Subcommittee, this completes my prepared statement. I would be pleased to respond to any questions you may have at this time.

[38]GAO, *Nuclear Weapons: NNSA and DOD Need to More Effectively Manage the Stockpile Life Extension Program*, GAO-09-385 (Washington, D.C.: Mar. 2, 2009).

[39]GAO, *Nuclear Weapons: Improved Management Needed to Implement Stockpile Stewardship Program Effectively*, GAO-01-48 (Washington, D.C.: Dec. 14, 2000).

GAO Contact and Staff Acknowledgments

If you or your staff have any questions about this testimony, please contact me at (202) 512-3841 or trimbled@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement. GAO staff who made key contributions to this testimony are Allison Bawden, Jonathan Gill, and Kiki Theodoropoulos, Assistant Directors; and Nancy Kintner-Meyer, Michelle Munn, and Jeff Rueckhaus, Senior Analysts.

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.

GAO's Mission	The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.
Obtaining Copies of GAO Reports and Testimony	The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's website (http://www.gao.gov). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to http://www.gao.gov and select "E-mail Updates."
Order by Phone	The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, http://www.gao.gov/ordering.htm. Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537. Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.
Connect with GAO	Connect with GAO on Facebook, Flickr, Twitter, and YouTube. Subscribe to our RSS Feeds or E-mail Updates. Listen to our Podcasts. Visit GAO on the web at www.gao.gov.
To Report Fraud, Waste, and Abuse in Federal Programs	Contact: Website: http://www.gao.gov/fraudnet/fraudnet.htm E-mail: fraudnet@gao.gov Automated answering system: (800) 424-5454 or (202) 512-7470
Congressional Relations	Katherine Siggerud, Managing Director, siggerudk@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548
Public Affairs	Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800 U.S. Government Accountability Office, 441 G Street NW, Room 7149 Washington, DC 20548

Please Print on Recycled Paper.

Mr. MURPHY. Thank you. We will go through these quickly.

I want to start off. Dr. Meserve, one of the messages from your work and General Alston's work is the lack of an embedded security culture from DOE headquarters on down through the various nuclear weapons complex facilities. As a former chairman of the Nuclear Regulatory Commission, you have experience with embedded safety culture. Am I correct on that?

Mr. MESERVE. That is correct.

Mr. MURPHY. And the lessons—what lessons, from your experience of NRC regulation of the civilian nuclear industry can apply to establishing strong security culture at DOE's facilities and operations? Can you give us an example?

Mr. MESERVE. Well, let me say that I think that perspective of the NRC has been that a safety culture is the critical foundation for ensuring the safe operations of the plants. That without that commitment, you have a problem that in regardless of how detailed the requirements are, ultimately you have to demand the people fulfill their obligations and take responsibility, and the safety culture, which is something that affects everyone in the plant, is the foundation.

So I came to this project with that perspective, and I think that, as has been mentioned, and General Alston emphasized this in his remarks, is that culture is the critical ingredient, and that is something that has to change to have something that will be sustained over time. People see this as responsible as their clear responsibility at every level at the facility and at headquarters.

Mr. MURPHY. And that is the same as sustained training for security personnel, I am assuming?

Mr. MESERVE. It means sustained training. It means a responsibility of everyone in the plant, when they see a problem, to raise that issue up. If their immediate supervisor doesn't take it up, it means going above that person. It means having a system in place so that no one is—faces any discipline or discrimination as a result of the fact that they have raised an issue like that. It is people to be rewarded if they take initiative to respond. And that is the sort of thing you need in the security area as well.

Mr. MURPHY. Thank you.

General Alston, you stated in your report that nuclear weapons sites leverage their unique missions and geography to justify a preferred, what you called "alone and unafraid" mantra, and that DOE and NNSA headquarters has employed a largely hands off response. What do you mean by "alone and unafraid?"

General ALSTON. Mr. Chairman, at Y–12 specifically, earlier in the year, earlier in calendar year 2012, the site security apparatus had upgraded their security system, and they—there was a multi-$100 million option, and this was still a very expensive option of, I can't remember, $60 to $70 million. And so they went forward with this $60 to $70 million modification to their overall security capability at the site, but when they deployed that capability early in the year, it had flaws that needed to be worked out, and that was widely known, but they operated anyway, generated hundreds of alarms, false alarms or nuisance alarms a month, conditioned the force, I would argue, to not respond with urgency because they were being conditioned that the alarms are systemic shortcomings.

There was—they moved towards the accounting for the alarms and less running to the sounds of the guns, which I think was manifested on the morning of July 28, because of the delayed response, because it was another false or nuisance alarm, if you will. And in that whole effort, though, was—from my perspective—was Y–12 saw a way to improve its security, and in my view, I saw evidence they conceived, designed, developed, and deployed this capability at Y–12, defending their unique geographical challenges to secure that facility, and in making their, if you will, one off approach to this, to be dominant between the relationship between Y–12 and the headquarters. And so there was not evidence of a strong, disciplined, central management of security modifications so that the field can, soup to nuts, take a look at what they determined to be shortcomings, and then worked the solution set on their own without what I think is more appropriate, a good operational test evaluation program where someone is accountable in the headquarters for the next gate you go, and that nobody lives with a sub-optimized system that is not operating perfectly on day one.

Mr. MURPHY. Is this systemic across NNSA?

General ALSTON. Well, we found a different approach at Pantex. I can't tell you the current state of this, so maybe Dr. Meserve can amplify this, but the ARGOS system, and I can't tell you what the acronym stands for, but it is a comprehensive security approach that is present at all of their sites. But depending on how you manipulate part of the overall ARGOS architecture at your particular site, they may not be precisely identical at each one of the facilities. So as these folks were trying to integrate the changes to their security apparatus and blend in to this ARGOS concept, there is so much freedom of movement at each one of the sites that I think there is great opportunity being missed trying to centralize common standards and force a common approach and making the sites defend being different than the common approach, as apposed to right now, which is give them the benefit of the doubt that they need to support the one off approach and that the common standards get subordinated to the unique approach. I don't know if I said that right.

Mr. MURPHY. Thank you. That helps a lot, but as this goes through, I can't help, as I am hearing these stories about security issues, too, of the people watching the radar on Pearl Harbor on December 7 said oh, pay no attention to those blips, that is just probably our planes coming over, or on 9/11. These things continue on, and hope that the security force is not going to just look past these things. I mean, to recognize a situation like this, as Mr. Meserve, you put in your letter that sometimes training of terrorists is to look nonthreatening, and you have to be ready for deadly force, and this could have ended up in a deadly situation, and we are hoping these things are avoided in the future.

I am out of time. I am going to go Ms. DeGette now from Colorado.

Ms. DEGETTE. Thank you very much, Mr. Chairman.

Mr. Trimble, when you were reciting the whole litany of problems that we have had with the various labs, it was like I was reliving my congressional career. So I want to ask you, have you read General Finan's report?

Mr. TRIMBLE. Yes, I have.

Ms. DEGETTE. And what is your opinion of her recommendations?

Mr. TRIMBLE. You know, all the recommendations sound sound. We have not done a full evaluation or anything of that nature. I think our reaction to the reports, as well as the actions DOE has already taken is sort of the proof is in the pudding.

Ms. DEGETTE. Yes, so you think it is a good direction, but you want to make sure it gets implemented?

Mr. TRIMBLE. Yes, and I think even more than that, it would be where is the implementation plan?

Ms. DEGETTE. Right.

Mr. TRIMBLE. So we have got a lot of oK, we are going to do this, we are going to do that, but where is the DOE summary of all of these efforts saying hey, this is our assessment of all this good work these people have done, and here is our plan with metrics and dates and who is accountable going forward.

Ms. DEGETTE. OK. And General, have you read General Finan's report?

General ALSTON. No, ma'am, I have not.

Ms. DEGETTE. OK.

General ALSTON. Her report was in draft while we were essentially commissioned by Secretary Chu.

Ms. DEGETTE. Are you familiar with her recommendations?

General ALSTON. I am familiar with a lot of them. I couldn't recite them for you.

Ms. DEGETTE. I am not asking you to. Good news, I only have 5 minutes.

So my question, though, is do you think she is going in the right direction with her recommendations, based on your assessments?

General ALSTON. I do. Where I was encouraged particularly by her approach was trying to certainly recognize the field shortcomings, but the headquarters chain——

Ms. DEGETTE. Right.

General ALSTON [continuing]. Needs to be fixed, and it needs a solid focus on it.

Ms. DEGETTE. It needs to be clarified, right?

General ALSTON. Absolutely.

Ms. DEGETTE. Yes, what about you, Dr. Meserve?

Mr. MESERVE. My response would be the same.

Ms. DEGETTE. OK. Now every few years—I alluded to this in my previous questioning. Every few years, some in Congress suggest that NNSA should be autonomous. From oversight last year, the House passed the National Defense Authorization Act that included a provision providing additional autonomy from oversight by this committee, for example, for NNSA. Luckily, this language was not in the final law and part of our job is to make sure that we have adequate oversight, so we are glad it wasn't in the final law. I think, and all of us on this committee think, the Y–12 security breach shows that the NNSA is simply not ready for that level of autonomy that the National Defense Authorization Act contemplated.

So General, I want to ask you and Mr. Meserve, were any of the issues you identified caused by a lack of autonomy for contractors

and those who worked for Y–12? Were they caused by a lack of autonomy?

General ALSTON. I would say that the consequence of the relationship between the semi-autonomous nature of NNSA and the Department of Energy did cause a conflict in ambiguity for policy, and so, the NNSA was dependent upon Department of Energy apparatus for independent inspection by HSS and the Inspector General properly so.

Ms. DEGETTE. So what you are saying is the autonomy that they had actually caused some of the problems?

General ALSTON. That they didn't have sufficient autonomy for them to be exclusively accountable for the failure.

Ms. DEGETTE. OK, and that was because they were partially reporting to DOE?

General ALSTON. Because the field would look up the chain of command, and there were limits to how beholden they were to the NNSA because certain policy elements were the purview and domain of organizations in the headquarters that were outside the——

Ms. DEGETTE. So it was because it wasn't fish or fowl, they were semi-autonomous, right?

General ALSTON. Yes, ma'am, and Dr. Meserve may have a better way to say this from our perspective.

Ms. DEGETTE. Dr. Meserve?

Mr. MESERVE. I think that part of the problem was not the autonomy of NNSA but the fact that there is a very confusing structure.

Ms. DEGETTE. Within the agency.

Mr. MESERVE. If something was simplified and then clear lines of authority and responsibility is what is necessary.

Ms. DEGETTE. Right.

Mr. MESERVE. That could be done with an autonomous NNSA. It could be done with the current structure, but having clear guidelines of who is in charge of what.

Ms. DEGETTE. The problem wasn't—yes, I got you. The problem wasn't whether it was autonomous or not, the problem was there wasn't a chain of command.

I want to ask you very quickly, Mr. Trimble, do you think that—does the GAO believe that NNSA's issues can be solved through a simple structural change?

Mr. TRIMBLE. We have previously testified that we do not. We think the issues that need to be addressed can be done with the current structure, and again, it is cultural changes, sustained effort.

Ms. DEGETTE. Thank you.

Mr. MURPHY. The gentlelady yields back.

Now recognize the gentleman from Ohio, Mr. Johnson, for 5 minutes.

Mr. JOHNSON. Thank you, Mr. Chairman, and gentlemen, thank you for being with us today.

Dr. Meserve, if the Department of Energy office responsible for independent oversight is subjected to political retaliation for conducting that oversight, how would that impact their ability to remain objective and independent, in your view?

Mr. MESERVE. Well I mean, the obvious danger is that if they are being criticized for doing their job that they will then back off doing what they are supposed to be doing. And so I think that that would be unfortunate, that if they didn't have a clear view of what their obligations were and their mission is.

Mr. JOHNSON. OK. General Alston, what is your view of the importance of independent oversight?

General ALSTON. I think that it is appropriately integrated in a mosaic of sensors and indicators to tell you how sturdy your readiness, or in this case, the quality of the security. I think that if you move too much towards depending on independent inspection and evaluation, you are missing great opportunity to have—to defend yourself against crisis. You are focused on defending against crisis and ultimate failure, but you are not taking advantage of building routine relationships and seeing whether or not your organization has the capacity to recognize failure when the conditions begin to present themselves. If you need someone outside to tell you how ready you are, you may not have the skill yourself to know yourself. So I believe it needs to be a mosaic of inputs that are converging at the right level to give the leadership at the local, intermediate, and the higher levels the competency and the confidence in just what the quality of the performance of the unit is.

Mr. JOHNSON. I couldn't agree with you more, and it is analogous to—I know in my 26½ year career in the Air Force, you have your unit mission, you have standards and evaluation who are the internal looks, eyes, and ears to make sure that you are following those rules, but you also have the Inspector General who takes a look from the outside, and both are very, very important.

Back to the issue, though, of political retaliation. To both of you, what impact would political retaliation have on safety and security, the culture of safety and security? You mentioned, Dr. Meserve, that people would just stop.

Mr. MESERVE. Well, you need to have a system that reinforces the priority that is to be given for safety and security, and that anything that interferes with the capacity for people to have a willingness to confront those issues honestly and to address them thoroughly is a detriment to achievement of safety and security. And that could be through political process, through fear of retaliation by a superior, there is any number of things that could affect it, but the point here is to keep your eye on the ball and anything that distracts you from that is a negative factor.

Mr. JOHNSON. Sure.

Mr. MESERVE. And I couldn't agree more with General Alston is that one ought not to anticipate that you are counting on oversight function as your primary means to prevent shortfalls. That responsibility has to be in the line organization that is responsible for the job, and they should be held accountable for it. The oversight is a protective mechanism to make sure that they are fulfilling their function adequately and appropriately.

Mr. JOHNSON. Absolutely.

General ALSTON. And sir, I would add just one point, and that is if you don't have at a grass roots level the kind of environment where the folks will come forward to expose weakness and challenge, you are not going to get to the self-critical culture—the level

of self-critical culture that you really need in this business where the stakes are so high.

Mr. JOHNSON. Yes, I couldn't agree with you more.

General, given the site's, I quote, "alone and unafraid" posture, how important, in your opinion, are standardization, benchmarking, and best practices to achieving and sustaining high security levels?

General ALSTON. Sir, clearly they feed every day. When you can, on a routine level, have the lines of communication sufficiently open where there is collaborative process, and standards don't have to be issued from above, there can be collaboration. It builds trust, it builds flow of information up and down the chain. Myself and Mr. Augustine came to the conclusion that the federalization of the correct protective force should be given serious consideration, and the reason—I am a unity of command guy, and that creates a seam with the operator, who is enriching uranium or whatever the other part of the mission would be, and so it is a little odd for me to have come down on this side. But for precisely the reasons of standardization and more centralized control and impact that I felt that that would be one means by which that could be achieved.

Mr. JOHNSON. Well thank you. Mr. Chairman, I actually do have one more question, if it would please the chair that I could ask it, otherwise I will yield back.

Mr. MURPHY. We will give you an additional minute.

Mr. JOHNSON. OK.

General Alston, one final question. General Finan's task force noted a distinct bias against finding and stating performance criticisms. You stated your belief that one of the attributes of a security organization is, and I quote, "an absolute intolerance for shortfalls, deficiencies, outages 1 minute longer than necessary." What must happen for NNSA to transition from General Finan's assessment to the attribute that you describe?

General ALSTON. I played an active role as the Air Force was recovering from its epic failures. I was required to produce a road map, and there were a lot—obviously we were on fire, and there were a lot of activities that had to go on there. But one of the things that we instituted was to find structural mechanisms to prove leadership commitment, and so the Chief and Secretary created a nuclear oversight board that met quarterly, and it was a forum where everyone with nuclear equities at the senior level would meet. But it was a forum where you could expose whatever level of detail that you wanted to expose, and in the case of the failure that we saw at Y–12, it wouldn't require so much the senior levels at NNSA, but there needs to be a process where the connection is reinforced so that you are tracking outages to the right level, and for example—or equipment shortages, and that there is a recurring forum so that routine interaction can fortify commitment to the security part of the enterprise.

Mr. JOHNSON. Thank you, General.

Mr. Chairman, I yield back.

Mr. MURPHY. All right, now recognize the gentleman from New York, Mr. Tonko, for 5 minutes.

Mr. TONKO. Thank you, Mr. Chair.

The obvious major part of NNSA's work is security, but equally important is providing their employees with a safe working environment. The consequences of safety failures are serious and for example, in October of '07, GAO reported that nearly 60 serious accidents or near-misses had occurred at NNSA's national labs since 2000. Just to give one example, GAO described a 2004 accident where a student working at the NNSA facility at Los Alamos was blinded in a laser accident.

Mr. Trimble, you had indicated in your testimony that GAO has been conducting assessments of safety at NNSA for quite some time, and while I heard some of the results being mentioned here, I am more—I would like to know, more importantly, how the agency is fairing. Are they getting better at addressing safety concerns?

Mr. TRIMBLE. I would like to say yes, but as of now, I can't say that our work is showing that. I think one of the things that is relevant to the discussion today that ties into the safety and security reform initiatives from 2010 is we have previously reported that those initiatives did not address our concerns previously expressed regarding the safety culture at NNSA and specifically, we noted that some of those reforms we viewed weakened federal independent oversight by making HSS's role sort of more of a "Mother, may I" in terms of being able to come in and inspect facilities. And I think in our testimony as well, we note since our last testimony on these matters in the fall, there have been numerous other safety incidents that have been reported. So our concerns necessarily continue.

Mr. TONKO. Thank you. You also made mention, and I will quote, that "they have not demonstrated sustained improvements in terms of their safety reforms." Can you tell us about NNSA's recent efforts to reform those measures in terms of safety protocols?

Mr. TRIMBLE. I don't know about protocols, per se. I think the 2010 safety initiative, the reform initiative, you did a lot to—there is a lot of good in there in terms of consolidating or rationalizing directives, et cetera. Again, as I noted, we saw problems with it, but as with security, the issue is one of sustainment. You go through these same periods of an accident happens, it gets attention, you have remedial measures, and then attention wanes and you go through the same cycle once again.

Mr. TONKO. So then what should the agency do or be doing to promote or improve worker's safety?

Mr. TRIMBLE. Well, I think again it is—one, it is a continued and sustained effort in addressing sort of a cultural issues that have crept in. I think you see, just as in security where you have the divide between headquarters and the field units, there is a divide there in terms of the importance and differing perceptions, perhaps, of the level of importance this sort of mission holds.

Mr. TONKO. And in terms of any oversight protections?

Mr. TRIMBLE. In terms of oversight? Well, independent—clearly, we haven't been on the record in terms of having robust independent oversight, much like in the security realm, so bolstering the role of HSS in that regard I think is essential.

Mr. TONKO. OK. I will yield back, Mr. Chair.

Mr. MURPHY. Thank the gentleman, and I want to say that for all the panelists, I thank you today, both panels. I also want to

note that certainly at times like this when we have hearings about security issues, security breaches, there are those who want to see where weaknesses are. They certainly take note of the comments made, and we recognize a lot of the things are being done for security remain certainly in the classified levels. But in a situation like this, I think it gives the ranking member and I and members of both sides of the Aisle confidence to know that actions are being taken, because in a world where terrorists on any level may take action against our interests at site such as this or other ones, that our Nation will be strong and stand up and prevent problems in the future with this. And so we thank you for your comments and good Americans to help us with that security.

I ask unanimous consent that the contents of the document binder and all the Majority memos be introduced into the record, and authorize staff to make appropriate redactions. Without objection, the documents will be entered into the record with any redactions the staff determines appropriate.

[The information appears at the conclusion of the hearing.]

Mr. MURPHY. And in conclusion, again, thank you to all the witnesses. I remind members they have 10 business days to submit questions for the record, and I ask all the witnesses agree to respond promptly to the questions.

This committee is now adjourned. Thank you.

[Whereupon, at 12:15 p.m., the subcommittee was adjourned.]

[Material submitted for inclusion in the record follows:]

5-17-10
MAY 17 2010
A > DOE
Mary
Peter's

The Secretary of Energy
Washington, D.C. 20585

May 5, 2010

The Honorable Joe Barton
Ranking Member
Committee on Energy and Commerce
U.S. House of Representatives
Washington, D.C. 20515

Dear Congressman Barton:

Thank you for your March 30, 2010, letter regarding the Department of Energy's (DOE) Safety and Security Reform Plan. First, let me assure you that we are committed to maintaining the highest standards of safety and security at our sites. DOE has conducted its nuclear operations for decades without a major accident and has long maintained worker injury and illness rates that are significantly below comparable industry standards. DOE also maintains a robust security protection posture for our nuclear sites, which has been rigorously tested to verify the capability to withstand the full range of postulated terrorist threats. Our management and operating contractors are responsible for safety and security performance, and we will continue to hold them directly accountable for achieving the safety and security requirements in their contracts.

The goal of our reform efforts is to fulfill our mission objectives more effectively and more efficiently. We view safety and security to be integral to those mission objectives. To that end, we are undertaking efforts to improve our safety and security directives and internal oversight processes. In our review of the Department's safety and security directives, we plan to maintain an appropriately robust set of regulatory-based and contractually applicable requirements, while eliminating redundant requirements. Further, we are refocusing our Federal oversight and enforcement efforts to more specifically target areas of greatest risk.

DOE's oversight of safety and security performance has not and will not diminish. The Office of Independent Oversight, within the Office of Health, Safety and Security (HSS), has undertaken numerous new activities that have actually increased its field presence and knowledge concerning site safety and security program performance. With respect to security, HSS will conduct an assessment at all facilities with Category 1 special nuclear material before the end of the calendar year.

As stated in the Reform Plan, the only oversight activities that have been suspended are those associated with lower risk standard industrial operations. Similarly, these are the only activities affected by the National Nuclear Security Administration's (NNSA) six-month moratorium on internally-driven assessments. Activities will continue to be subjected to local monitoring by DOE and NNSA site offices on an as-needed basis and

Printed with soy ink on recycled paper

will be subjected to independent oversight when site performance requires increased attention (e.g., for-cause reviews and regulatory enforcement actions).

Shifting independent oversight resources previously devoted to these activities has increased the resources available to assist line managers in tackling difficult challenges and solving problems that have remained unresolved by layers of duplicative oversight in the past. For NNSA, shifting its resources will allow DOE to develop an integrated and comprehensive oversight approach and devote needed resources to ensuring that contractors are implementing effective assurance systems. Our efforts have already resulted in significantly increased communication and cooperation among all departmental elements.

We are currently conducting a series of congressional committee briefings on our reform goals and activities. Glenn Podonsky, the Department's Chief Health, Safety and Security Officer, is working to schedule a briefing with the Energy and Commerce Committee's minority staff to provide additional information on implementation of the Department's Reform Plan.

If you have any questions, please have your staff contact Betty A. Nolan, Senior Advisor, Office of Congressional and Intergovernmental Affairs, at (202) 586-5450.

Sincerely,

Steven Chu

cc: The Honorable Michael C. Burgess
Ranking Member
Committee on Energy and Commerce
Subcommittee on Oversight and Investigations
U.S. House of Representatives

The Honorable Henry A. Waxman
Chairman
Committee on Energy and Commerce
U.S. House of Representatives

The Honorable Bart Stupak
Chairman
Subcommittee on Oversight and Investigations
U.S. House of Representatives

Department of Energy
National Nuclear Security Administration
Washington, DC 20585

DEC 13 2012 ACT-NA-72-12-12-2012-484945

MEMORANDUM FOR DISTRIBUTION

THRU: MICHAEL K. LEMPKE
ASSOCIATE ADMINISTRATOR
FOR INFRASTRUCTURE AND OPERATIONS

FROM: SANDRA E. FINAN, BRIG GEN, USAF
ACTING ASSOCIATE ADMINISTRATOR
FOR DEFENSE NUCLEAR SECURITY

SUBJECT: Directive Rescission and Impact Assessment

This memorandum rescinds direction and suspends actions being taken in response to the attached memorandum dated August 31, 2011, *Direction for Recently Issued Departmental Orders for Certain Safeguards and Security Program Areas.* We intend to execute a deliberate process to restore the Department of Energy (DOE) directives as the baseline safeguards and security policy for the National Nuclear Security Administration (NNSA) and this is an important first step. This direction applies to all NNSA contracts to include contracts managed through the Office of Acquisition and Supply Management, but does not apply to NNSA Headquarters (i.e., District of Columbia and Germantown). The directives that are currently on the contracts will remain until the Office of Associate Administration for Management and Budget provides a formal notification.

Executing this transition effectively will require collaboration among the Headquarters, Federal Site Offices, and the contractor community. As we implement this initiative, we need to fully understand the impact on our partners across the nuclear security enterprise before modifying any contracts. We request that you conduct an impact assessment and report your results.

Please identify issues that will have a measurable cost or significant operational impact on your implementation of the following DOE Orders:

(A) 470.4B, *Safeguards and Security Program*, July 21, 2011;

(B) 473.3, *Protection Program Operations*, June 27, 2011 (Attachments 1 and 2, Federal and Contractor Protective Force); and

(C) 474.2, *Nuclear Material Control and Accountability*, June 27, 2011.

Printed with soy ink on recycled paper

Your impact responses should address the following two elements:

(1) Describe any significant issues that would result from implementing the current DOE directives, including cost impacts. Identify specific areas where implementation of current DOE directives will require an implementation plan beyond a six-month implementation. Please include page, section, and paragraph number cross-references for the current DOE Orders and existing contract directives that support your issues.

(2) Describe your proposed resolution to address any significant issues caused by implementing the current DOE Orders, including potential use of equivalencies and exemptions processed in accordance with DOE O 251.1C, *Departmental Directive Program* January 15, 2009.

By January 31, 2013, please report your assessment of the costs and schedule for implementing the DOE Orders to DNSCorrespondence@nnsa.doe.gov. Inquiries regarding this direction should be referred to Mr. Larry Small, Office of Field Support, at (202) 586-1412.

Attachment

Distribution: Jeffery Harrell, NA-15
Douglas Ash, NA-74
Mark Holecek, KCSO
Kevin Smith, LASO
Kimberly Davis, LSO
Steven Erhart, NPO-1
Stephen Mellington, NSO
Douglas Dearolph, SRSO
Geoffrey Beausoleil, SSO

cc: Neile Miller, NA-2
James McConnell, NA-00
Joseph Waddell, NA-APM-10
Don Cook, NA-10
Catherine Tullis, NA-MB-20
Frank Lowery, NA-70
Catherine McCulloch, NA-70.1
Paul Saunders, NA-71
Donald Stout, NA-72
Robert Osborn II, NA-IM-1
Wayne Jones, NA-IM-1
Laurel Hautala, KCSO
Michael Duvall, LASO

3

Duane Gordon, LSO
Gary Wisdom, NPO-20
Raeford Phifer, Jr., NSO
Roxanne Jump, SRSO
Eileen Johnston, SSO

ATTACHMENT

Department of Energy
National Nuclear Security Administration
Washington, DC 20585

August 31, 2011

MEMORANDUM FOR DISTRIBUTION

FROM: DOUGLAS E. FREMONT
CHIEF, DEFENSE NUCLEAR SECURITY

SUBJECT: Direction for Recently Issued Departmental Orders for Certain Safeguards and Security Program Areas

Recently, the Department of Energy (DOE) issued several new Orders pertaining to the Safeguards and Security Program, specifically DOE Order (O) 470.4B, *Safeguards and Security Program,* dated July 21, 2011; DOE O 474.2, *Nuclear Material Control and Accountability*, dated June 27, 2011; DOE Standard 1194 2011 for *Nuclear Material Control and Accountability*, dated June 2011; and DOE O 473.3, *Protection Program Operations,* dated June 27, 2011. As with all new directives, sites have six months to either meet all new requirements or develop and approve implementation plans toward that end.

Subject matter experts from the nuclear security enterprise (NSE) have been working together to develop and promulgate specific National Nuclear Security Administration (NNSA) security policies. The NNSA Policy Letters (NAPs) which correspond with the above referenced Departmental Orders are near completion and should be ready in the near future. Therefore, NNSA sites should not take action to conduct an impacts assessment of the new Orders or place them on the site contracts. The existing Orders should remain on the site contracts until the respective NAP is issued by the Administrator and placed on the site contracts. This direction also extends to Federal entities located outside of the Washington D.C. metro area and possessing and non-possessing contractors managed out of the Office of Acquisition and Supply Management.

The draft NNSA *Program Planning and Management* NAP is in the review process within NNSA at this time and we anticipate it to be published within the next few months. We are currently working on the draft Protection Program Administration NAP, which is also expected to be issued in the near future. Both of these NAPs will replace DOE O 470.4B. Likewise, the draft NAP for Nuclear Material Control and Accountability is in the final coordination process and is also expected to be promulgated before the end of the year, and will replace DOE O 474.2.

The new DOE O 473.3 establishes requirements for three separate topical areas: Physical Protection, Contractor Protective Force, and Federal Protective Force. The Physical

Printed with soy ink on recycled paper

Protection requirements in DOE O 473.3 were replaced by NAP 70.2, *Physical Protection,* in June 2010. The draft NAP for Protective Force, which provides requirements for contractor protective forces, is in the final stages of development and will replace DOE O 473.3, Attachment 2, *Contractor Protection Force.* Due to the complexity of the revision to 10 Code of Federal Regulations (CFR) 1046, we cannot guarantee that this NAP will be promulgated this year. We expect the draft 10 CFR 1046 will undergo the rulemaking process shortly and anticipate its completion in the near future allowing us to finalize the NNSA Protective Force NAP. Therefore, DOE O 473.3, Attachment 2, should not be implemented at this time. If the rulemaking process takes longer than anticipated, our office will reevaluate. Finally, our office does not have responsibility for Federal Protective Forces and we will therefore not be addressing those requirements in DOE O 473.3.

As we continue our efforts to develop additional NNSA policies for the other security topical areas, there will be more opportunities to tailor and streamline the Defense Nuclear Security requirements program to our mission and operations. I appreciate your continued support through this process to ensure that we achieve the greatest benefits in terms of cost savings and increased operational efficiencies from this effort while maintaining an effective security program.

If you have any questions or wish to discuss this matter further, please call Mr. Kevin Leifheit, Director, Office of Field Support (NA-72), at (202) 586-4400, or Mr. Michael Bodin (NA-72) at (202) 586-7610.

Distribution: Joseph Waddell, NA-APM-10
Mark Holecek, KCSO
Alice Williams, LSO
Kevin Smith, LASO
Stephen Mellington, NSO
Jeffrey Harrell, OST
Steve Erhart, PXSO
Douglas Dearolph, SRSO
Patty Wagner, SSO
Theodore Sherry, YSO

cc: Donald Cook, NA-10
Kevin Leifheit, NA-72
Larry Wilcher, HS-50
Laurel Hautala, KCSO
Daune Gordon, LSO
Pamela Valdez, LASO
Raeford Phifer Jr., NSO
Mark Jackson, OST
Gary Wisdom, PXSO
Carroll McFall, SRSO
Roxanne Jump, SRSO
Eileen Johnson, SSO
Donat St. Pierre, YSO

The Deputy Secretary of Energy
Washington, DC 20585

March 16, 2010

MEMORANDUM FOR KRISTINA M. JOHNSON, UNDER SECRETARY OF ENERGY
STEVEN E. KOONIN, UNDER SECRETARY FOR SCIENCE
THOMAS P. D'AGOSTINO, UNDER SECRETARY FOR NUCLEAR SECURITY
GLENN S. PODONSKY, CHIEF HEALTH, SAFETY AND SECURITY OFFICER
INGRID A. C. KOLB, DIRECTOR, OFFICE OF MANAGEMENT
SCOTT BLAKE HARRIS, GENERAL COUNSEL

FROM: DANIEL B. PONEMAN

SUBJECT: Department of Energy 2010 Safety and Security Reform Plan

The Department has recently developed the attached end-state vision for safety and security reform, which will guide our efforts to enhance productivity and achieve the Department's mission goals while maintaining the highest standards of safe and secure operations at Department of Energy facilities. It is imperative that we initiate the necessary actions quickly to attain this end state in 2010.

In 2009, the Office of Health, Safety and Security (HSS) began reforming its approach to enforcement and oversight by recognizing line management's responsibility for safety and security, reviewing opportunities for streamlining requirements, and eliminating directives that do not add value to safety and security. I have tasked HSS to continue this reform path, but they will need your input, cooperation and support. Therefore, please assure that senior managers and key staff from your Headquarters and field organizations are working closely with HSS to achieve our common goals.

The attached Plan outlines actions and milestones that require your attention. I recognize that this is a major effort and will involve the timely commitment of valuable resources, but your support, as well as input from the Defense Nuclear Facilities Safety Board and our stakeholders, is vital to our success.

Success will be measured through near-term relief from specific low-value burdensome requirements as well as longer-term streamlining of requirements that will lead to measurable productivity improvements. Please keep me informed of our progress and to alert me in a timely manner of any impasse that needs my attention.

Attachments

Printed with soy ink on recycled paper

cc: Ines Triay, EM-1
William Brinkman, SC-1
Pete Miller, NE-1
James Markowsky, FE-1
Cathy Zoi, EE-1
David Geiser, LM-1
Mike Weis, PNSO, FMC Chair
Jeff Smith, ORNL, Deputy Director
Al Romig, SNL, Deputy Director
Adam Cohen, PPPL, NLDC Executive Secretary

Attachment 1

End-State Vision for Safety Reform

To enhance productivity and achievement of mission goals, while maintaining the highest standards of safe operations at DOE facilities through the development, implementation, and assurance of effective, streamlined, and efficient safety policies and programs.

Safety Performance: Contractors are provided the flexibility to tailor and implement safety programs in light of their situation without excessive Federal oversight or overly prescriptive Departmental requirements.

Safety Responsibilities: To facilitate effective mission accomplishment, decision-making authorities are pushed to the lowest appropriate level of contractor and Federal management, considering hazards, risks, and performance history. Authority and accountability for safety rests with line management, including responsibility for and oversight.

Safety Requirements: DOE worker safety requirements are based upon existing national standards, with internally-derived requirements developed to address unique DOE conditions. DOE's regulatory requirements for occupational safety and health are founded on regulations promulgated by the Occupational Safety and Health Administration (OSHA), invoke current national standards to address outdated aspects of OSHA regulations, and establish or invoke requirements to address unique DOE workplace hazards. The Department's corporate approach for maintaining the highest standards of safe operations is promoted through its Integrated Safety Management Policy, DOE P 450.4, *Safety Management System Policy*, and implemented by contractors through Department of Energy Acquisition Regulation Clause 970.5223-1, *Integration of Environment, Safety and Health into Work Planning and Execution.*

Safety Assurance: The Department's contractors maintain an assurance system that provides reliable measurement of the effectiveness of their safety management systems and facilitates timely corrective actions to system or performance weaknesses.

Regulatory Oversight and Enforcement: HSS's approach to safety regulatory oversight and enforcement supports line management's efforts to affect the conduct and priorities of their contractors. Oversight is focused on safety performance. Oversight inspections and enforcement actions are prioritized for contractors with poor safety records and serious or recurring violations, and are consistent with approaches and penalties employed by OSHA and the Nuclear Regulatory Commission.

Attachment 2

End-State Vision for Security Reform

To enhance productivity and achievement of mission goals, while protecting sensitive information, technologies, and materials through the development, implementation, and assurance of effective, streamlined, and efficient security policies and programs.

Security Performance: Contractors are provided the flexibility to tailor and implement security programs in light of their situation and to develop corresponding risk- and performance-based protection strategies without excessive Federal oversight or overly-prescriptive Departmental requirements.

Security Responsibilities: To facilitate effective mission accomplishment, decision-making authorities are pushed to the lowest appropriate level of contractor and Federal management, considering vulnerabilities, risks, and performance history. Authority and accountability for security rests with line management, including responsibility for oversight.

Security Requirements: DOE security strategies are based upon legally mandated requirements, national standards developed by peer agencies, a rational threat assessment, and internally derived requirements developed to address unique DOE security risks. DOE-unique security requirements are streamlined, non-redundant, focused on desired performance outcomes, and tailored to specific mission and site risks. DOE security requirements are standardized where necessary to support interoperability and cost savings.

Security Assurance: The Department's contractors maintain an assurance system that provides reliable measurement of the effectiveness of their security programs and facilitates timely corrective actions to system or performance weaknesses.

Regulatory Oversight and Enforcement: HSS's approach to independent oversight and regulatory enforcement supports line management's efforts to affect the conduct and priorities of their contractors. Oversight is focused on security performance. Oversight inspections and enforcement actions are prioritized for contractors with serious or recurring violations of security requirements, with penalties commensurate with potential harm to national security and with those imposed by peer agencies.

Attachment 3

DOE 2010 SAFETY AND SECURITY REFORM PLAN

Background

In 2009, the Office of Health, Safety and Security (HSS) began working to reform its enforcement and oversight approach, recognizing line management's significant responsibility for safety and security. To date, this approach has resulted in (1) increased coordination of enforcement actions with line management, (2) working with the Field Management Council (FMC) to understand where reform in its oversight and enforcement practices is needed, (3) suspending independent oversight of low-hazard operations and lower-value security assets, except for those cases where site performance requires increased attention, and (4) maintaining rigorous and informed oversight of high-hazard operations or high-value security assets.

In November 2009, following the safety and security reform studies directed by the Deputy Secretary, HSS began a disciplined review of all HSS directives, including a systematic review of the Department of Energy safety and security regulatory model (which includes both DOE directives and regulations). As a result, HSS identified 24 directives for potential cancellation (subject to consultation with the Program Offices, including the Central Technical Authorities). HSS has also developed approaches for safety and security disciplines that are expected to result in more than a 50 percent reduction in the number of existing safety and security directives for which HSS is the Office of Primary Interest.

Priority Actions and Milestones

The Department is setting the following safety and security reform goals and target milestones. The Department leadership team expects senior managers of Headquarters and field organizations actively to support these challenging efforts. Specifically, leadership of each Headquarters and field organization will need to ensure the timely and efficient engagement of appropriate managers and staff at all levels of the organization as needed to support HSS in achieving the actions listed below.

Action	Milestones
Process: Initiate directives process changes to support the pace of this reform effort and require a rapid (3-day) escalation for impasse (veto) resolution.	March 2010
Outreach: Develop an outreach plan that will engage, inform and enlist the support of DOE internal and external stakeholders, (including the Defense Nuclear Facilities Safety Board) throughout this reform effort to achieve our end-state vision. Outreach includes a roundtable discussion with the Deputy Secretary, Under Secretaries, and various worker unions in March.	March 2010
Security Near-term: Provide relief from specific burdensome security	March 2010

requirements by: 1) finalizing approval of the revised Unclassified Controlled Nuclear Information Order, 2) issuing a policy memorandum on Foreign Visits and Assignment, and 3) submitting a revised Accountable Classified Removable Electronic Media (ACREM) policy for Departmental review.	
Near-term cancellations: Initiate the Departmental review process to cancel the unneeded directives with the goal of completing the cancellations in April.	March 2010
Oversight and Enforcement: Redefine the HSS independent oversight and regulatory enforcement functions to achieve the end-state vision to include submitting a revision of DOE Order 470.2B, Independent Oversight and Performance Assurance Program for Departmental review.	May 2010
Worker Safety: Streamline the Department's worker health and safety, Integrated Safety Management, and Oversight directives for submittal for Departmental review. Pursue further identification of issues with the Department's worker safety regulations, 10 CFR 851 (that will then be evaluated through the rule making process).	May 2010
Classification: Streamline the Department's classification and information control directives within 90 days following the publication of the pending executive order (E.O.) for Controlled Unclassified Information and the President's Information Security Oversight Office (ISOO) implementing directives for E.O. 13526, Classified National Security Information.	Milestones based on the issuance of the E.O.
Environmental Management: Integrate the Department's environmental management and energy management directives, including adoption of ISO 14001 as the Department's standard for environmental management and the requirements of E.O. 13514 into one order for submittal for Departmental review by April. Also, due to the benefits achieved from Departmental review already conducted, complete the revision and issuance of the Radiation Protection of the Public and the Environment Order (DOE O 458.1) as scheduled in July.	July 2010, with interim milestones in April as specified
Quality Assurance: Streamline the Department's Quality Assurance directives for submittal for Departmental review.	July 2010
Operating Experience: Streamline the Department's operational experience and feedback directives into an integrated operational awareness and risk management approach for submittal for Departmental review.	August 2010
Nuclear Safety: Recognizing the importance of the Department's nuclear safety regulations and directives, a review will be conducted to clarify the existing relationship between regulation- and directive-driven requirements, address any identified gaps in requirements, and reduce unnecessary burden where there is no commensurate safety benefit. The review will be completed and the revised directives will be submitted for Departmental review by September. As part of this effort, the Defense	September 2010, with interim milestones in May as specified

Nuclear Facility Safety Board will be consulted. Also, due to the benefits achieved from Departmental review already conducted, complete the revision and issuance of the four nuclear safety orders currently in Departmental review (DOE O 425.1D, DOE O 433.1B, DOE O 422.X, and DOE O 426.Y) as scheduled in May.	
Security: Streamline the Department's safeguards and security directives by leveraging the National Nuclear Security Administration Zero-Based Security Review (ZBSR) to update all related Departmental directives, by October, including submitting a revised Safeguards and Security policy for Departmental review in March and the updated Safeguards and Security Program order for Departmental review in June.	October 2010, with interim milestones in March and June as specified

HENRY A. WAXMAN, CALIFORNIA
CHAIRMAN

JOE BARTON, TEXAS
RANKING MEMBER

ONE HUNDRED ELEVENTH CONGRESS

Congress of the United States
House of Representatives
COMMITTEE ON ENERGY AND COMMERCE
2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6115

Majority (202) 225-2927
Minority (202) 225-3641

March 30, 2010

The Honorable Steven Chu
Secretary
U.S. Department of Energy
1000 Independence Avenue, S.W.
Washington, D.C. 20585

Dear Secretary Chu:

We are writing with regard to a "Department of Energy 2010 Safety and Security Plan" recently reported in the press and described in a March 16, 2010, memorandum sent from the Department of Energy (DOE) Deputy Secretary Daniel Poneman to DOE senior management. According to Deputy Secretary Poneman, since 2009 the Department's Office of Health, Safety and Security has been taking steps to reform its approach to enforcement and oversight of safety and security at DOE facilities. The objective of the plan appears to be to provide contractors with the flexibility to tailor and implement safety and security programs without excessive federal oversight or overly prescriptive Departmental requirements.

As you are aware, the Government Accountability Office (GAO) has conducted extensive reviews in the past relating to safety and security compliance at DOE sites. As GAO has documented in numerous reports and testimony before the House Energy and Commerce Committee, DOE has experienced significant challenges in the past managing effectively the many billions of dollars appropriated to the agency and the multiple projects which DOE is directed to carry out in both the civilian and defense areas. These challenges include documented concerns that DOE federal site offices, responsible for the day-to-day oversight of DOE contractors, may not have sufficient personnel with the necessary skills to manage and oversee effectively the work being performed by contractors at their sites. At the same time, contractor self-assurance and assessment systems may also be inadequate and/or not yet well developed to meet many of the Department's tasks.

Post 9/11 reforms and a series of incidents the Committee investigated over the past decade at Los Alamos National Laboratory, Lawrence Livermore National Laboratory, and

elsewhere focused needed attention on and prompted improvements in safety and security during the past Administration. Given the long history of DOE's management challenges and the grave safety and security risks within the nuclear weapons complex, it is imperative that DOE ensure safety and security-related improvements that are currently in place can continue and be sustained and that DOE be cognizant of lessons from past incidents and management failures. In light of this, we have concerns particularly about whether, and the extent to which, DOE should be taking steps now to outsource safety and security measures to contractors without strong federal oversight.

To address our concerns, we sent the attached request to GAO today to ask for its assistance in evaluating the Department's ongoing reform plan and related activities. In addition, we request that the Department (i) provide our Minority Committee staff with a briefing on the "Department of Energy 2010 Safety and Security Plan" and all related activities; and (ii) provide a written response with full information regarding any enforcement or oversight activities relating to safety and security that have been suspended during the past year, and assurances that suspension of those activities does not raise any security-related concerns.

Thank you for your prompt attention to this matter. If you have any questions related to this request, please contact Mr. Alan Slobodin of Minority Committee staff at (202) 225-3641.

Sincerely,

Joe Barton
Ranking Member

Michael C. Burgess
Ranking Member
Subcommittee on Oversight and Investigations

Attachment

HENRY A. WAXMAN, CALIFORNIA
CHAIRMAN

JOE BARTON, TEXAS
RANKING MEMBER

ONE HUNDRED ELEVENTH CONGRESS

Congress of the United States
House of Representatives
COMMITTEE ON ENERGY AND COMMERCE
2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6115

Majority (202) 225–2927
Minority (202) 225–3641

March 30, 2010

Mr. Gene L. Dodaro
Acting Comptroller General
U.S. Government Accountability Office
441 G Street, N.W.
Washington, D.C. 20548

Dear Mr. Dodaro:

Over the past year, Department of Energy (DOE) Secretary Steven Chu has initiated or supported a number of significant changes in the priorities, management and direction of the Department, including initiatives that relate to agency oversight at some of the nation's most sensitive national security facilities. In connection with these efforts, on March 16, 2010, Deputy Secretary Daniel Poneman issued a memorandum to DOE senior management describing initiatives the Department has taken to reform its approach to enforcement and oversight of safety and security, including at National Nuclear Security Administration (NNSA) facilities within the nuclear weapons complex.

The memorandum describes a "Department of Energy 2010 Safety and Security Reform Plan" and provides an "end-state vision" for such reforms and a schedule for plan implementation to be completed this year (see Attachment). The objective of the plan, as reflected in the end-state vision, appears to be to provide contractors with the flexibility to tailor and implement safety and security programs without excessive federal oversight or overly prescriptive Departmental requirements.

We write to request your assistance in evaluating DOE's ongoing safety and security reform plan and related activities. We have received reports that during the past year as part of its reform initiative:

- DOE's Office of Health, Safety and Security has suspended some independent inspections of DOE and NNSA facilities within the nuclear weapons complex;
- NNSA has suspended dozens of internal reviews and assessments; and

- NNSA and the Office of Science are implementing an oversight model at some of their sites that relies less on direct federal oversight and more on contractor self-assessment.

DOE carries out many of the nation's most critical national security-related missions, including stewardship of the nation's nuclear weapons stockpile and the environmental remediation of the Cold War era nuclear weapons complex. As the Government Accountability Office (GAO) has documented in numerous reports and testimony before the House Energy and Commerce Committee, DOE has experienced significant challenges over the years in managing effectively the many billions of dollars appropriated to the agency and implementing all of the multiple projects which DOE is directed to carry out in both the civilian and defense areas. These challenges include documented concerns that DOE federal site offices, responsible for the day-to-day oversight of DOE contractors, may not have sufficient personnel with the necessary skills to manage and oversee effectively the work being performed by contractors at their sites. At the same time, contractor self-assurance and assessment systems may also be inadequate and/or not yet well developed to meet many of the Department's tasks.

Post 9/11 reforms and a series of incidents the Committee investigated over the past decade at Los Alamos National Laboratory, Lawrence Livermore National Laboratory, and elsewhere focused needed attention on and prompted improvements in safety and security during the past Administration. Given the long history of DOE's management challenges and the grave safety and security risks within the nuclear weapons complex, it is imperative that DOE ensure safety and security-related improvements that are currently in place can continue and be sustained and that DOE be cognizant of lessons from past incidents and management failures. In light of this, we have concerns particularly about whether, and the extent to which, DOE should take steps now to outsource safety and security measures to contractors without strong federal oversight. Accordingly, we request that GAO undertake a review of these reform initiatives with a focus on the following questions:

1. What is the factual justification and basis for embarking on these reforms and the management model or approach DOE senior management relies upon to drive these high-level initiatives?
2. What types of efforts have NNSA and DOE program and oversight offices launched in response to the Department's ongoing safety and security reform initiatives, and what is their implementation status?
3. What independent oversight activities relating to safety and security have been suspended as DOE has pursued its safety and security reform initiatives, and does the suspension raise any safety or security concerns?
4. Based on current progress and on the large body of work compiled by GAO, the DOE Inspector General, and a variety of DOE- and Congressionally-appointed commissions, what is the likelihood of success for the Department's current safety and security reform initiatives, and where might the Congress most usefully direct its oversight resources?

We request that GAO focus its efforts on NNSA because of its extensive contracting and project management activities and critical national security role and functions. In addition, we also request that GAO focus on DOE's Office of Health, Safety and Security, because we have

particular concerns about the implementation of the Secretary's initiatives in that office, which plays a key role in overseeing security and safety of DOE and NNSA operations.

Thank you for your assistance with this matter. If you have any questions, please contact Mr. Alan Slobodin with the Committee Minority staff at (202) 225-3641.

Sincerely,

Joe Barton
Ranking Member

Michael C. Burgess
Ranking Member
Subcommittee on Oversight and Investigations

cc: The Honorable Henry A. Waxman, Chairman

The Honorable Bart Stupak, Chairman
Subcommittee on Oversight and Investigations

Attachment

Assessment of NNSA Federal Organization and Oversight of Security Operations

National Nuclear Security Administration

OFFICIAL USE ONLY
May be exempt from public release under the
Freedom of Information Act (5 U.S.C. 712),
exemption number category: Exemption 7-Law Enforcement
Department of Energy review required before public release.
Name/Org: Norbert Marcelle, NA-70
Date: November 7, 2012

Department of Energy
National Nuclear Security Administration
Washington, DC 20585

MEMORANDUM FOR THE ADMINISTRATOR

FROM: SANDRA E. FINAN, BRIG GEN, USAF
SECURITY TASK FORCE LEAD

SUBJECT: Transmittal of Task Force Report on the Assessment of NNSA Federal Organization and Oversight of Security Operations

Following the July 28, 2012, security incident at the National Nuclear Security Administration's (NNSA) Y-12 National Security Complex, a Task Force was commissioned on August 14, 2012, to analyze the current federal NNSA security organizational structure and security oversight model and recommend possible improvements. I was appointed to lead this Task Force. The Task Force was directed to:

- Analyze current NNSA security organizational structure and recommend possible improvements that would improve operational focus, oversight, and culture sustainment.
- Analyze current NNSA security oversight model and mechanisms to determine what seams exist and what structures could be implemented to better ensure that the issues are found and fixed before they become problems.

The attached report documents the results of our analysis and our recommendations. It is important to note two key points:

- The items documented in this report are remarkably similar to those documented in previous reports. NNSA has been resistant to the kind of organizational, cultural, and operational changes that would put security on a sustainably sound footing.
- Although outside the charter of the Task Force, the role of leadership is crucial and must be taken into account when considering the report findings.

While the report highlights negative aspects of the NNSA security organization and assessment model, the Task Force found many great people on the NNSA security staffs. They are clearly dedicated, skilled, and hard-working and want to get the security mission done right. Unfortunately, NNSA security personnel see themselves thwarted by lack of management support and feel obstructed by some of their peers. Their difficulties are compounded by the absence of a workforce strategy to recruit, retain,

Printed with soy ink on recycled paper

and develop a cadre of talented, knowledgeable and experienced security professionals. Thus, it is all the more encouraging that these personnel, almost without exception, genuinely care about doing good work. Their continuing strong desire to build a successful security organization is a hopeful sign for the future.

Attachment

Table of Contents

1. INTRODUCTION 2
1.1 Task Force Mission 2
1.2 Major Results 3
2. ORGANIZATION 5
2.1 Introduction 5
2.2 Discussion 8
2.3 Findings 9
3. ASSESSMENT 14
3.1 Introduction 14
3.2 Discussion 14
3.3 Findings 16
4. RECOMMENDATIONS 19
4.1 Overarching 19
4.2 Organization 20
4.3 Assessment 22
5. PROPOSED ORGANIZATIONAL STRUCTURE 23
6. PROPOSED ASSESSMENT MODEL 26
7. CLOSING 28

APPENDICES:

A. Task Force Charter
B. Task Force Team Composition
C. Task Force Methodology
D. Alternative Organizational Structures
E. Other Observations
F. Selected Bibliography

1. INTRODUCTION

1.1 TASK FORCE MISSION

In the aftermath of the July 28, 2012 security incident at the National Nuclear Security Administration's (NNSA) Y-12 National Security Complex, the leadership of the NNSA and the Department of Energy (DOE) took action to address the security failures at Y-12. The initial information gathered revealed that issues at Y-12 were part of a larger pattern of security program management deficiencies.[1] These security issues prompted the NNSA Administrator to commission[2] a Task Force to analyze the current Federal NNSA security organizational structure and security oversight model and recommend possible improvements.[3] The NNSA Administrator directed the Task Force to:

- Analyze current NNSA security organizational structure and recommend possible improvements that would improve operational focus, oversight, and culture sustainment.
- Analyze current NNSA security oversight model and mechanisms to determine what seams exist and what structures could be implemented to better ensure that the issues are found and fixed before they become problems.[4]

While other reviews were aimed at diagnosing the root causes of the Y-12 event, the NNSA Administrator's direction called for this Task Force to focus on the "path forward" within the Federal NNSA organization. Under the leadership of Brigadier General Sandra Finan, USAF, the Task Force consisting of NNSA, DOE, and military specialists conducted extensive document reviews and interviewed Federal managers and staff as well as a selection of contractor security managers and others across the NNSA security organization.[5] The Task Force collected and analyzed information, identified issues, and herein proposes solutions. Sections 2 and 3 of this Report present and discuss the findings under the headings of Organization and Assessment.[6] Section 4 presents recommendations based on the findings. Section 5 presents a proposed approach to an NNSA security organizational structure that addresses operational focus, oversight, and culture sustainment. Section 6 presents a proposed approach to an NNSA security oversight model to better ensure that issues are found and addressed before they become problems. Section 7 presents the Task Force's closing. Supporting information is presented in the appendices.

---

1) In the context of the Task Force Report the phrase "security program" encompasses security-related functions and activities across the NNSA in addition to budget line funding.
2) NNSA Charter, Assessment of NNSA Federal Organization and Oversight of Security Operations, Thomas P. D'Agostino, NNSA Administrator, August 14, 2012. (Appendix A)
3) The actual delivery of security and other services in NNSA is performed by contractors. The Federal security organization manages the work of these contractors and assesses their performance.
4) The term "seam" in the Charter is understood to include gaps, overlaps, and organizational friction points.
5) The Task Force team composition is provided in Appendix B. The data collection methodology is detailed in Appendix C.
6) The term "oversight" in DOE and NNSA usage has both the usual, generic meaning and a specific reference to the "independent oversight" role of the DOE Office of Health, Safety, and Security (HSS). The term "assessment" is more commonly used to describe such programs within NNSA. To avoid confusion, the Report therefore generally uses the term "assessment" to refer to NNSA-specific programs, and "oversight" to refer to the HSS programs.

1.2 MAJOR RESULTS

The Task Force noted significant deficiencies in security organization, oversight, and culture sustainment throughout the NNSA security organizations. In the NNSA security organizations, line management authority is ill-defined and claimed by multiple Federal organizations. The term "line management authority" as used in this Report, is the "ability to direct others to execute elements of the security mission." It does not refer to typical staff functions such as the development of requirements and promulgation of policy. On the one hand, the "Federal field organizations" exercise line management authority over the site security contractors via the contract management structure.[7] On the other hand, the NA-70 asserts that it also has such authority. Absent clearly defined lines of authority, many individuals assert authority, while correspondingly few have been assigned responsibility. This lack of clear lines of authority contributes to a widespread practice of decision-making by consensus. When consensus fails, organizational elements can act independently or not at all, which undermines effective implementation of the security program. Conflicting interpretations of the NNSA Act itself add to the confusion.[8]

The Task Force further noted a significant gap in the current NNSA security organizational structure. At the strategic level the Headquarters organization has been ineffective and has intervened in field tactical execution.[9] The Federal field organizations have been ineffective in performing their tactical responsibilities for executing the security program and have intervened in strategic matters. Additionally, there is no clearly identified operationally-focused organization that bridges the gap between strategic and tactical responsibilities and addresses standardization, field execution, and multi-site analysis.

The Task Force found a broken security performance assessment model. It also found that NA-70 came to rely overwhelmingly upon Federal staff simply reviewing contractor-provided data, rather than effectively assessing performance itself. At the same time the DOE Office of Health, Safety and Security (HSS), which is responsible for independent oversight, had been directed as part of governance reform, to reduce the frequency and rigor of its reviews of NNSA. Of particular concern is the observation that potentially critical management information is not being reported clearly to the appropriate decision makers.

As concerning as these structural and assessment issues might be, the most striking result of this review falls in the area of culture sustainment. It quickly became evident that the Task Force findings closely resemble those presented in numerous prior reports such as the

7) The term "Federal field organization," as used in this report, refers primarily to the NNSA site offices, but also includes the recently created Nuclear Production Office which functions as a consolidated site office for the Y-12 and Pantex sites as they move toward a single consolidated contract structure.
8) NATIONAL NUCLEAR SECURITY ADMINISTRATION ACT [As Amended Through P.L. 111–383, Enacted January 7, 2011]
9) As referenced in this Report, the "strategic" level develops long range planning and goals to ensure proper execution for achieving end results, the "operational" level implements the overall strategy by giving direction to tactical elements and providing support to reach mission objectives, and the "tactical" level performs day-to-day operations and oversight to ensure that duties and tasks are being completed.

2005 Mies Report and the 2004 Chiles Report.[10] While NNSA has attempted to correct some identified issues over the years, it has not adequately emphasized effective security mission performance. In recent years, NNSA security leaders have chosen to emphasize security cost containment to the detriment of security program execution. The idea that the requirements for security performance effectiveness are subordinated to cost concerns has become a prevailing concept in the NNSA security community. This emphasis has become endemic throughout the NNSA security culture, so much that fundamental facility protection issues such as the protection of ongoing operations came to be regarded as too expensive and therefore "out of bounds" for analysis.[11] The NNSA security culture has focused on fiscal limitations over effective performance. This has resulted in an environment in which deficiencies are worked at the margins rather than management addressing core issues.

These issues underscore the critical role of effective leaders. While outside the charter of this Task Force, it must be acknowledged that leadership plays the key role in mission accomplishment. The Task Force recognized that effective leadership may compensate for structural deficiencies within an organization; however, restructuring alone cannot overcome leadership shortcomings. The best assessment model is useless if leaders fail to effectively implement it. Additionally, the assessment model will not be effective unless leaders consistently demand comprehensive, unbiased information. NNSA must take ownership of its history of security failures. Leadership must take bold and enduring actions if this pattern is to be broken.

10) See Appendix F, Selected Bibliography for the full citation of these reports and other related materials.

11) For example, highly enriched uranium operations at Y-12 were suspended for 18 days following the security breach. The Task Force found that continuity of operations was not a significant factor in the planning and execution of the site security program.

2. ORGANIZATION

2.1 INTRODUCTION

The current NNSA security organizational structure is confusing in terms of the relationships between the NNSA Administrator, Office of Information Management (NA-IM), the newly established Office of the Associate Administrator for Infrastructure and Operations (NA-00), Office of Defense Nuclear Security (NA-70) and the Federal field organizations. There is an intermingling of statutory, programmatic, line, and staff functions within the NNSA security organization.

The primary NNSA Headquarters security organization is the Office of Defense Nuclear Security (NA-70), which reports directly to the NNSA Principal Deputy Administrator. The NA-70 Director is also the Chief of Defense Nuclear Security (CDNS). The Chief of Defense Nuclear Security position is established in the NNSA Act and has a reporting line to both the NNSA Administrator and the Secretary of Energy. The authority to appoint the Chief of Defense Nuclear Security resides with the Secretary of Energy, and is exercised with input from the NNSA Administrator. The NA-70 Director reports to the NNSA Principal Deputy Administrator, and as the Chief of Defense Nuclear Security has direct access to the Secretary of Energy--this creates two lines of communication.

Separate from the formal mission and functions of NA-70, the Chief of Defense Nuclear Security position is also designated by the Secretary of Energy and NNSA Administrator as the Cognizant Security Authority (CSA) for NNSA. This authority can be further delegated. Federal officials that are delegated CSA authority can commit security resources or direct the allocation of security personnel or approve security implementation plans and procedures in the accomplishment of specific work activities.

NA-70 has four offices. Security Operations and Performance Assessment (NA-71), Field Support (NA-72), Nuclear Materials Integration (NA-73), and Personnel and Facility Clearances (NA-74). Additionally, NA-70 has a Resource Management staff (NA-70.1) and an Intelligence and Counterintelligence Liaison function (NA-70.2). See Figure 1.

Federal field organizations are structured for execution of the NNSA security program in many different ways. Some security organizations report to the senior field manager, while others do not. Some organizations are singularly focused on the security mission while others are part of a more diverse portfolio that could include business operations, project management, etc. The diversity of organizational structures has the effect of working against the initiative to achieve NNSA-wide consistency, standardization of policy, training, and program implementation. This blurs roles, responsibilities, and line management authority.

Line management authority runs from the NNSA Administrator through NA-00 to the Federal field organization managers and their security staffs, and finally to the contractor who executes the mission. CSA flows from the NNSA Administrator to the Chief of Defense

Nuclear Security directly to the Federal field organization leadership and currently may be further delegated. The Chief of Defense Nuclear Security exercises security line management authority to direct Federal security staff and extends this to the contractors. Thus, the Chief of Defense Nuclear Security and Federal field management concurrently exercise line management authority, causing conflict and confusion. While the CSA is a line management authority, it does not follow the same delegation path as other line management authorities, compounding this confusion.

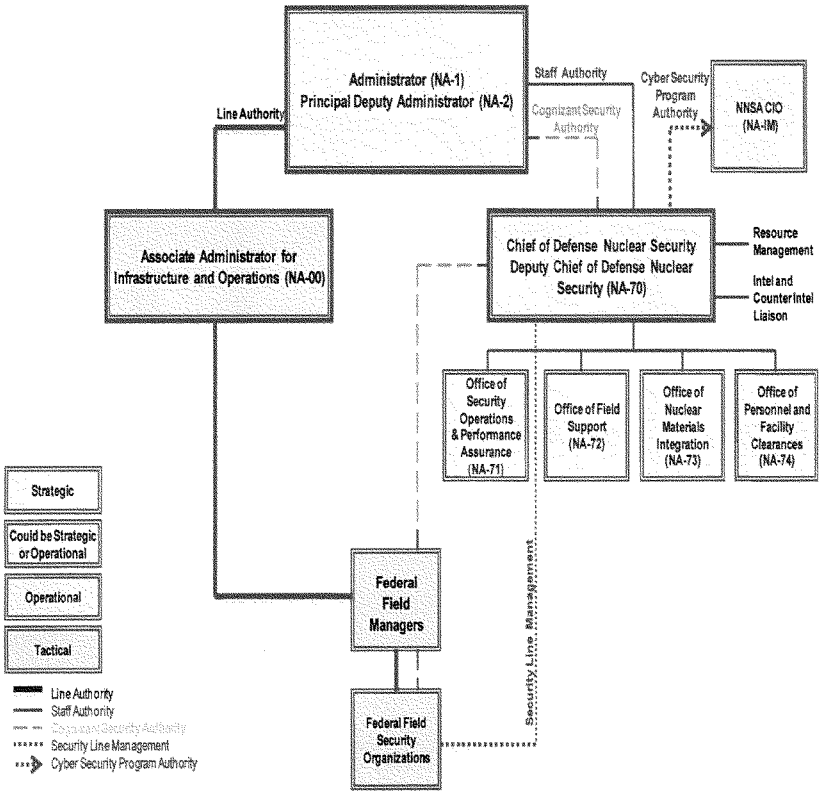
The Task Force noted a significant organizational weakness that is due to a gap in the NNSA security structure. The Headquarters security function is basically strategic, providing policy, guidance, and requirements. The Federal field organization role is fundamentally tactical, executing the day-to-day security program. The NNSA lacks an operational level to communicate strategic policy and requirements as guidance that supports NNSA-wide standardization, to provide technical assistance to individual field organizations, and to perform other functions that are field-oriented and multi-site in character and application. This shortcoming contributes to Headquarters becoming involved in tactical-level line management decisions, and for tactical-level managers to assert a strategic role.

Noticeably absent from the above discussion are the NNSA Program Offices. Until recently, the Federal field organizations reported to the Deputy Administrator for Defense Programs (NA-10). This has changed so that they now report to the Associate Administrator for Infrastructure and Operations (NA-00). Neither organization has any formal role in the development and implementation of the NNSA security program, although each "owns" the security staffs at the Federal field organizations, budgeting for their salaries and benefits and assuming responsibility for their professional development and training.

HSS also plays a role in the NNSA security program. In addition to being the office of primary interest for DOE Security Orders, it performs independent oversight of NNSA Headquarters and field locations. HSS is also responsible for providing basic corporate security education and professional development through the National Training Center.

Figure 1

Current NNSA Security Organizational Structure



2.2 Discussion

The existing NNSA security organizational structure is convoluted and ineffective. The Task Force observed that lines of authority in virtually every organizational function are divided. The NNSA security function is not well organized or effectively staffed and the NA-70 policy development and implementation process is broken. While the Chief of Defense Nuclear Security is the Cognizant Security Authority (CSA), this responsibility has been unevenly delegated and is open to inconsistent interpretation. Security staffs are responsible to multiple lines of authority and for some functions may not be responsible to anyone. The most fundamental issues arise from the relationship between NA-70 and the Federal field organizations. NA-70 believes that it has line management authority over the security elements within the Federal field organizations. However, the managers of these field organizations have been formally assigned line management authority. The NNSA Act states that the Chief of Defense Nuclear Security role includes "the development and implementation of security programs". The current interpretation of this provision has been a source of ambiguity due to the mixing of line and staff responsibilities in a single organization.

Roles and responsibilities are either undefined or not followed. The Task Force identified numerous occasions across the NNSA security organizations where individuals are not allowed to perform assigned duties or assume roles and responsibilities nominally assigned to others. The confusion of roles and responsibilities is evident in NA-70, within field organizations, and between NA-70 and the field. For example, the approved mission and function statements for NA-71 and NA-72 have little apparent relationship to the way these offices operate and how they interact with each other or with the NA-70 "front office." Within field organizations, the Task Force noted a number of instances where management precludes staff from performing the assigned roles of their position and/or assigns personnel to unrelated duties. At times, NA-70 acts as a formal line management organization, and asserts responsibilities that are formally assigned to the Federal field security organizations. NA-70 personnel are frequently frustrated by site-level resistance to the programmatic direction they provide and Federal field security managers are often similarly frustrated when NA-70 uses its budget authority, its control over the policy process, and other activities to inject itself into what the sites regard as their line management decision-making process.

There are no clear lines of authority. There are overlapping lines of authority and a mixing of staff and line functions. The CSA function flows from the NNSA Administrator through the Chief of Defense Nuclear Security to the Federal field organizations. Line management authority goes from the NNSA Administrator through the Associate Administrator for Infrastructure and Operations (NA- 00), to the field. However, NA-70 attempts to exert line management authority and provides programmatic guidance directly to the Federal field security managers. While Federal field organizations administer the contracts governing the actual performance of the security mission, NA-70 routinely interacts with the security

contractors. Furthermore, NA-70, not the line managers, is the primary executer of the NNSA security budget.

The security policy process is broken. The Task Force identified that there is no clearly articulated or consistently implemented NNSA security policy process. A major concern is the supplanting of DOE Security Orders with generic and less restrictive NNSA policies (NAPs). This appears to be based on a desire to reduce funding demands through a reduction of requirements. Additionally, the Task Force noted a desire on the part of some NA-70 senior managers to maximize separation from DOE HSS policies and activities. Within NA-70, policy and guidance are issued through a variety of formal and informal mechanisms with erratic distribution. The Task Force identified that some Federal field organizations are inconsistent in their acceptance and application of NA-70 issued policies. Finally, NA-70 policy and guidance tend to be vague resulting in widely differing interpretations by field personnel.

The NNSA Federal security organization is not effectively structured or staffed. While there are clearly strategic (Headquarters) and tactical (Federal field organizations and contractors) levels, there is little indication of an effective operational element with responsibility for security program functions such as site assistance and standardization of program execution. The Task Force also noted that the Federal field organizations structure their security functions substantially differently. This results in a lack of standardization of both organization and execution of the security program. At some sites there is weakening of the security function and reduced senior management attention. There are a number of personnel issues associated with the security professional staff, including the lack of a human capital development plan, no career path, and limited mobility. Additionally, the Task Force noted an overreliance on support service contractors who primarily assist the NA-70 organization.[12]

2.3 FINDINGS

2.3.1 Roles and responsibilities are either undefined or not followed.

2.3.1.1 Within NA-70 there is a lack of clearly defined and understood functions and missions. Despite approved mission and function statements within NA-70, there is uncertainty, inconsistency, and conflict between the NA-70 "front office", NA-71 and NA-72. The placement of NA-73 in the organization seems an anomaly that can divert senior management attention from the core security mission.

12) These support service contractors are distinct from security contractors who perform program functions such as protective forces.

2.3.1.2 **NA-70 has failed to implement a requirements-driven budget formulation process.** There is no clear delineation of responsibilities within the NA-70 organization between the requirements process and the budgeting process. There has been an overwhelming tendency, especially at Headquarters, for security requirements to be downwardly adjusted. The NA-70 leadership chose to lessen requirements rather than seek appropriate funding levels necessary for effective program execution. This has led to a wholly budget-oriented focus rather than a balanced approach in which requirements drive the process and senior management directs the balance between program execution and risk acceptance.

2.3.1.3 **The relationship between NA-70 and Federal field security staff is dysfunctional.** The roles and responsibilities for Federal staff are not clearly defined, understood, or consistently applied. The distinction between line management responsibility and Headquarters staff responsibility is blurred and negatively impacts the relationship between Headquarters and the field. This lack of clear roles and responsibilities has led to conflict between some Federal field security personnel and NA-70 (and sometimes a three-cornered conflict involving contractor security staff). There is also a cultural issue between some Federal field organizations and NA-70 in which communication with NA-70 security subject matter experts (SMEs) is actively discouraged and impeded by Federal field management. Some Federal field organizations assert that they "do not work" for NA-70. There are disagreements over who has responsibility, authority and accountability. As a result, Federal security organizations act to "protect turf" and are biased against sharing information. This has reduced the effectiveness of the NNSA security program.

2.3.2 **No clear line of authority within the NNSA security organization.**

2.3.2.1 **There is no clear line of authority.** There is no documented or consistent implementation of security responsibility and authority. The formal line management authority for executing security programs in the field does not include NA-70, the Chief of Defense Nuclear Security. However, the Federal field security managers have an informal 'dashed line' relationship to NA-70. This relationship intermingles line and staff functions, which has adversely impacted the communications between the Contracting Officer and the security contractor. The confusion has contributed to a degradation of mission performance, a lack of standardization in program implementation, inconsistent performance assessment, and has diluted senior management awareness of security operations, issues and risks.

2.3.2.2 Delegation of CSA is ill-defined and inconsistent. There is no clear policy guidance on what can be delegated or how the delegations are to be implemented. NAP- 70.2, *Physical Protection*, has allowed for varied interpretations of what can and cannot be delegated. There is no standardized process for the delegation of CSA from the Chief of Defense Nuclear Security to the Federal security managers. Further delegation of CSA to the security contractor is inconsistently exercised and in some cases inappropriate. As a result, the contractor is sometimes allowed to approve security plans and procedures without effective Federal oversight or approval.

2.3.3 NNSA security policy process is broken.

2.3.3.1 NA-70 has assumed responsibility for generating security policy without allocating adequate resources to ensure effective policy formulation. NNSA generated security NAPs as an alternative to following DOE security policy. NA-70 staffed its policy process by borrowing resources from other NNSA security functions, usually at the cost of disrupting the orderly performance of those other functions. The result has been that NNSA security policy formulation and issuance is incomplete, ad hoc, inconsistent with DOE security policy, and imperfectly communicated to the line organizations.

2.3.3.2. NA-70 has not clearly defined the necessary security program performance baseline. There is no clearly established requirements-driven baseline to govern the implementation of the NNSA security program and against which the program is assessed. Rather, the NA-70 approach deliberately departed from key DOE Security Orders and established a less restrictive security policy framework through the NAPs without resolving the different performance measurement expectations between the two policies. The lack of clearly defined performance requirements results in inconsistent and incomplete security program implementation.

2.3.4 NSA Federal security function is not properly organized or staffed.

2.3.4.1 **There is no standard or consistent organizational structure for security functions at the Federal field organizations.** The Federal field organizations carryout their security functions in different ways. While one size does not fit all, effective security organizations should have a set of core functions common across the security program. Currently, there is a lack of standardization and an uneven implementation of the Federal security program requirements. In some cases security functions are combined with other, non-security functions, taking management focus off of security program execution.

2.3.4.2 **The NNSA security organization has no operational-level element.** NA-70 primarily focuses on the strategic level of security, while the Federal field organization focuses on the tactical level. This leaves a gap at the operational level; there is no effective capability to provide implementation guidance or standardization and no one above the tactical level is appropriately focused on field operations. Without this operational focus each Federal field organization and each contractor is allowed to develop its own procedures for organizing and conducting security. The result is a fragmented and inconsistent execution of the NNSA security mission.

2.3.4.3 **The NNSA security functions are not staffed effectively and there is no human capital strategic plan.** While there is a technical qualification program for some security professionals, there is no formal strategy for the recruitment, retention, and appropriate progression of Federal security professionals. Current practice relies heavily on Headquarters' use of a cadre of support service contractors, in lieu of developing Federal security professionals with multi-site and/or multi-security discipline experience. The result is that Federal security staff may have limited opportunity for professional growth and often feel they are in a 'dead end' job.

2.3.4.4 **The NA-70 leadership overly relies upon support service contractors.** The senior NA-70 leadership has relied excessively upon contractors to provide core expertise. For example, the Security Operations Division's on-site workforce is two-thirds support service contractors. The other divisions' on-site workforce consists of an average of about 50% support service contractors. In addition, there is a very large number of other support service contractors used for field assistance activities. This overreliance on contractors, combined with the underutilization of the Federal work force, has contributed to the lack of an effective and sustained career path for Federal security professionals. Demoralization and feelings of disenfranchisement are evident in the Federal security workforce.

2.3.4.5 **NA-70 has not developed a program to integrate both local and national intelligence into daily operations at each of the specific sites.** There are no clear and effective organizational relationships with the Intelligence and Counterintelligence communities that provide consistent access at each organizational level to security threat and risk-relevant information. As a result, NA-70 and most Federal field organizations do not have effective intelligence support.

3. ASSESSMENT

3.1 INTRODUCTION

The Task Force expended considerable effort attempting to describe, understand and analyze the current assessment model and mechanisms. Currently, the NNSA security assessment model consists of three levels: 1) contractor self-assessments against policy, program and contractual requirements, 2) Federal field organization shadowing and evaluation of specific performance testing and program activities and also evaluation of the overall effectiveness of the contractor's self-assessment system , and 3) NA-70 evaluation of both the contractor's self-assessments and the effectiveness of the Federal field organizations' oversight activities. Additionally, periodic independent comprehensive security inspections of NNSA sites are performed by HSS.

There are issues with the implementation of the assessment activities at each of these levels. Some portions of the assessment process are not fully documented, some portions are not always followed, and other assessment activities appear to be locally improvised. To the extent that there is a security program baseline, it is derived from DOE Security Orders and NNSA security NAPs. However, there are significant unresolved inconsistencies between DOE Security Orders, NNSA NAPs, and a variety of narrowly focused local criteria. The NNSA NAP approach in security has been less specific and less defined than the approach specified in DOE Security Orders. NAP-21, *Transformation Governance and Oversight Initiative*, as interpreted by the NNSA security organizations, has enabled the contractors to determine how security programs are to be implemented and assessed. This extends to a belief that Federal oversight should be non-intrusive. There are no clearly established comprehensive performance standards or measurement criteria for the security program. NA-70 has not clearly communicated program guidance and performance expectations regarding NAP implementation. There is insufficient and incomplete training in the assessment process. Finally, constraints at both the field and NA-70 levels push Federal assessment activities firmly in the direction of mere paperwork reviews.

The Task Force recognized there are some aspects of the current assessment process, which should be fundamental to any assessment process with a large portion of the concerns focus on assessment program execution rather than on assessment program design. Additionally, there are structural aspects of the program that are causes for concern. The Task Force observed an endemic culture that accepts the current abdication of effective Federal program assessment as a given.

3.2 DISCUSSION

The failure to adequately assess security system performance and to clearly and unequivocally report deficiencies to the appropriate senior managers has been identified as a significant contributing cause to the Y-12 security incident. The Task Force focused upon

the performance assessment process as implemented by Federal field and Headquarters organizations within NNSA. Although contractor self-assessments are the first-line elements in the security performance assessment process, these were outside the direct scope of the review. Strengthening the contractor self-assessment process is an important objective, but cannot replace a rigorous Federal assessment process.

NNSA does not have an adequate security performance assessment process or capability. The performance assessment capabilities of Federal security organizations within NNSA are virtually non-existent. Essentially all responsibility for performance assessment is delegated to the Federal field organizations. The current Federal field organizations are typically limited to "shadowing" contractor self-assessments and/or reviewing the reports these self-assessments generate. Moreover, there is a tendency on the part of some field Federal staff to adopt the role of defending "their" contractors rather than attempting to objectively assess contractor performance. At the Headquarters level, the NA-70 performance assessment function has only three full-time Federal staff members. The Task Force noted that the current NA-70 assessment process is largely confined to the review of submitted paperwork. The result is that there is no NNSA Federal organization that is capable of performing effective security performance assessment.

The "systems-based" assessment model as implemented is ineffective for security. Misinterpretation, and/or misapplication of the DOE Safety and Security Reform Plan, dated March 16, 2010, resulted in a weakened Federal security assessment program. In particular, this document stated: "Security Performance: Contractors are provided the flexibility to tailor and implement security programs in light of their situation and to develop corresponding risk- and performance- based protection strategies without excessive Federal oversight or overly-prescriptive Departmental requirements." This guidance was further expanded upon and eventually articulated in NAP-21, *Transformation Governance and Oversight Initiative*.[13] The belief arose that "eyes on, hands off" precluded Federal security staff from conducting performance-based assessments of contractors. As a result, most Federal assessment is based on paperwork generated by the contractor. This paper-based system of assessment, without sufficient performance verification, is inadequate for effective evaluation of security operations.

NNSA has no clear and consistent performance baseline for security program implementation. A performance baseline, set forth in detailed standards and criteria, is the keystone of an effective security program. Precisely articulated standards and criteria further provide an objective foundation for performance assessment. Currently, NNSA does not have the standards or criteria necessary to effectively measure security program performance. The absence of such standards and criteria diminishes the ability to identify potentially significant performance deficiencies. The Task Force noted that the lack of

13) NAP 21, Chapter 8 states, "Line oversight activities are largely systems-based in functional areas of lower risk and where the contractor has demonstrated good performance..." Security programs at sites with special nuclear material, critical infrastructure, and/or other high value assets and activities are by definition of higher risk and therefore NAP 21 systems-based approach should not be applicable.

standards and criteria has been coupled with the widespread notion that contractors must only be told "what" the mission is, not "how" the mission is to be accomplished. While this approach may be appropriate in other areas, it is ineffective as applied to security programs. Therefore, security tasks are not necessarily performed in a manner consistent with NNSA security requirements.

The current assessment process is biased against criticism. The Task Force noted a distinct bias against finding and stating performance criticisms. HSS was asked to reduce the rigor and frequency of NNSA oversight. The NNSA Federal assessment relies heavily on contractor self-assessment. While an important tool, contractor self-assessments tend to be insufficiently objective. The primary Federal assessment role is performed by field staff. Long-term geographic proximity to site contractors can compromise the objectivity of these Federal assessors. Moreover, the intermingling of management and assessment roles within Federal field organizations can also contribute to less objective assessment. The NA-70 Headquarters performance assessment process, being paper-based, cannot validate the information submitted. Information provided to the Task Force suggests that in some instances information considered to be unfavorable is being "watered down" or obscured. Furthermore, information was presented that indicate differing opinions are being suppressed by some senior managers in the field and at Headquarters. As a result, NNSA senior leadership may not receive all information needed to make quality decisions.

3.3 FINDINGS

3.3.1 NNSA does not have an adequate security performance assessment capability.

3.3.1.1 NA-70 does not have an effective security assessment capability. The current paper-based assessment process is heavily dependent on field office and contractor reporting and does not include independent observation or validation of site security implementation. As a result, NA-70 is unable to validate the implementation of security policies or contractor performance of assigned missions.

3.3.1.2 NNSA Federal field organizations do not have consistently effective security assessment processes. The current process of reviewing contractor self-assessments and operational awareness activities does not provide adequate insight into contractor performance. In some cases Federal security staff has been limited to reviewing only contractor-provided paperwork. Consequently, Federal field organizations have become overly reliant on contractor-generated data in assessing contractor performance. Objective assessment of contractor performance can be compromised by day-to-day interactions. As a result, Federal field organizations cannot always validate contractor performance.

3.3.1.3 **NA-70 has virtually abdicated all responsibility for security assessment to the field organizations.** NA-70 leadership has provided little unifying direction to Federal field security staff. This has allowed for widely varied implementation of security assessment requirements. As a result, consistently effective security assessments are lacking, cross-site trends are not appropriately identified, and NNSA leadership is deprived of an appropriate program-wide understanding of the security program implementation.

3.3.1.4 **NA-70 has moved away from performance-based Federal security assessment.** The Federal security staff has only limited capability to do on-site assessments and has increased its reliance on contractor-provided data. NA-70 receives extensive paperwork, which is prepared by the contractors and transmitted by the Federal field organizations with their input. The excessive quantity of paperwork and questionable quality of the data, coupled with the Headquarters' inability to assess actual performance, precludes validating the information in the documents. This reliance on a paper-based approach has taken Federal security managers out of an active role in assessing actual security performance.

3.3.2 **The systems-based assessment model as implemented is ineffective for security.**

3.3.2.1 **The current implementation of systems-based assessments fails to uncover problems.** The current systems-based approach unduly emphasizes the contractor assurance process rather than actual performance results. This has largely replaced previous performance-based (transactional) evaluation. The Federal staff at Headquarters does not conduct any performance testing. While some Federal field organizations conduct performance testing on a limited basis, the current assessment approach discourages active Federal performance testing. As a whole, performance testing in the field has been of questionable effectiveness. Therefore, NNSA does not have an effective Federal capability to identify issues, and may be unaware of significant problems prior to their realization.

3.3.3 There is no clear and consistent performance baseline for program implementation.

3.3.3.1 NA-70 wrote and implemented policy documents, which were less restrictive than DOE policy and were subject to excessive interpretation. NA-70 produced NAPs, and other policy direction, that reduced security requirements and did not provide implementation guidance to clarify or build upon DOE security requirements. While the NAPs have allowed sites the freedom to tailor security programs to their specific needs, these NAPs also led to an absence of standardization and/or consistent implementation of security requirements. This lack of a standard baseline has the potential to place assets at risk. It also makes implementation of an integrated NNSA security program very difficult.

3.3.3.2 NA-70 did not establish standards and criteria that define expectations for security operations within NNSA. There is no comprehensive definition of security performance requirements. Consequently, there are no standards and criteria against which to measure the performance of NNSA security program execution at individual field locations or for the overall security program. The employment of such standards and criteria increases the ability to identify potentially significant performance deficiencies.

3.3.4 Current assessment process is biased against criticism.

3.3.4.1 Contractor self-assessments are insufficiently critical. The Task Force noted an unwillingness to report deficiencies through the contractor self-assessment process. The assessment process as currently applied avoids probing areas of potential weakness. The current NNSA contracting model insufficiently addresses critical self-assessment as an effective part of fee determination.

3.3.4.2 Federal field assessments are insufficiently critical. Long-term geographic proximity to site contractors can compromise the objectivity of the Federal assessors. Similarly, Federal field level involvement in local operational decisions can also limit objectivity. At some field locations management impedes the ability of Federal staff to effectively or thoroughly review contractor performance.

3.3.4.3 NA-70 does not have mechanisms to correct biases in assessment information. Information considered to be unfavorable is being "watered down" or obscured at NA-70 and lower levels. As a result, NNSA senior leadership may not be getting the information necessary for quality decision-making.

4. RECOMMENDATIONS

The following recommendations address findings noted in this Report. The Task Force identifies the first three recommendations as overarching, and believes these should receive priority attention. Specific organizational and assessment recommendations then follow.

4.1 OVERARCHING

4.1.1 Build and execute an NNSA Security Road Map that consolidates recommendations, articulates a clear vision of where the security program is going, and charts a path forward.

4.1.1.1 Evaluate this Report, and other security reports, in building a sustainable path to success. Document the path in a roadmap that is signed by the NNSA Administrator and follow up with action plans that have clear ownership, and status updates. Make the solutions enduring so that they are not again written up in the next report.

4.1.2 Restate and stress the role of security within NNSA to emphasize a stronger security focus and culture that embraces security as integral to the overall mission.

4.1.2.1 Leadership must emphasize the importance of the security mission in strategic plans, mission statements, policy documents, and other expressions of management intent. Security must be clearly integrated with other mission elements and appropriately recognized as essential to overall NNSA mission success.

4.1.3 NA-70 senior leaders must focus on the primary responsibility of developing an effective security program for the NNSA.

4.1.3.1 NA-70 needs to concentrate on its primary mission of producing a current and comprehensive NNSA security program. The security program scope must reflect the balance between requirements and fiscal realities. Ensure that budget constraints do not inappropriately influence the establishment of program requirements.

4.1.3.2 An effective security program for the NNSA must not only address the protection of special nuclear material and classified matter, but must also address other considerations such as continuity of operations and a broader spectrum of threats. NA-70 must clearly define the requirements that will serve as a basis for risk acceptance decisions by line management.

4.2 ORGANIZATION

4.2.1 Clearly define and document the roles and responsibilities across NNSA security functions.

4.2.1.1 Each organization needs to have clearly defined responsibilities. With each of these responsibilities the appropriate authority must be accorded. With responsibility and authority in alignment, individual and organizational accountability is established.

4.2.1.2 Propose a clarification to the NNSA Act that more effectively addresses clear roles and responsibilities for the Chief of Defense Nuclear Security and the security line management responsible for executing the NNSA security program.

4.2.2 Establish a clear Security line of authority.

4.2.2.1 Eliminate the bifurcation of the security line of authority for implementing security programs. The Chief of Defense Nuclear Security should develop appropriate policy guidance, but allow the CSA to flow from the NNSA Administrator through the NA-00 function to the Federal field organization managers. Create a clear distinction between line and staff functions.

4.2.3 Retain the CSA authority at the Federal level.

4.2.3.1 Clarify CSA delegation of authority and its limitation, so that it cannot be re-delegated to contractors.

4.2.4 Create an operational-level security organization that is responsible for the implementation and standardization of security operations in the field.

4.2.4.1 The operational-level organization should focus on standardizing security operations, ensuring that the security program is effectively executed, addressing NNSA-wide trends and issues, and ensuring that the requirements, budget and policy guidance appropriately meet the security needs of the field elements.

4.2.5 Establish an assessment capability that evaluates implementation of security programs across NNSA.

4.2.5.1 In order to ensure the security program is appropriately implemented across NNSA, this capability must include the ability to assess the performance of the Federal field security organization as well as that of the contractor.

4.2.6 Establish an appropriate Headquarters-level security policy capability.

4.2.6.1 Policy development and implementation is a Headquarters core function that requires a dedicated professional policy staff to execute. Whether writing stand-alone policy or articulating implementation instructions for higher level policy, this function is essential for security program execution.

4.2.7 Ensure that NA-70 security personnel have the appropriate level of security background, experience, and skill to properly carry out the NNSA security mission.

4.2.7.1 NNSA needs the right security professionals in the right places. Individual leaders and collectively the entire staff must possess an appropriate skill and experience base to provide effective security program execution. With the right team in place, Federal security leaders and staff can set a path to success.

4.2.8 Develop and execute a comprehensive human capital management program for Federal security professionals.

4.2.8.1 NA-70 leadership must take responsibility to create a comprehensive personnel management plan that develops current security professionals, prepares them for positions of broader scope or greater responsibility and recruits, and retains security talent needed to sustain the Federal security capability.

4.2.9 Reduce reliance on support service contractor personnel.

4.2.9.1 Support service contractors should be used to provide discrete products and services as defined in the statements of work. They should not be used as an alternative for appropriately skilled and experienced Federal staff.

4.2.10 Eliminate the conflict between DOE Security Orders and NNSA NAPs.

4.2.10.1 NNSA should use the DOE Security Orders. DOE has a specialized security policy function that produces its orders. Rather than attempt to duplicate this function, use the orders for direction and the NAP process to provide guidance and clarify information in the orders as appropriate, but not reduce requirements.

4.2.11 Implement a requirements-driven security budget formulation process.

4.2.11.1 Develop a structured planning, programming, budgeting, and execution process that ensure requirements are adequately stated and risks appropriately accepted.

4.3 Assessment

4.3.1 Implement a comprehensive, multi-tiered, performance-based security assessment process.

4.3.1.1 Implement an objective system in which performance information is identified, documented, and communicated, as appropriate.

4.3.1.2 Establish an effective Federal performance testing element in the security program assessment process.

4.3.1.3 The assessment program should include a comprehensive look at all security topical areas on a regular basis.

4.3.2 Establish clear security performance expectations (standards and criteria) and performance measures.

4.3.2.1 Develop and issue specific standards against which security operations are to perform and the criteria by which they will be evaluated. Consider inclusion of periodic and end of year performance evaluation requirements, fee strategy, and fee recommendations for security contractors.

4.3.2.2 Revisit governance reform as it applies to the security program. Ensure that appropriately stringent standards and criteria for performance are articulated in policy and program direction.

4.3.3 Revalidate and update the security performance requirements to ensure all levels of the threat spectrum are addressed.

4.3.3.1 Greater consideration of lower-level and non-traditional threats such as active shooters and protesters must be appropriately incorporated into performance requirements.

4.3.4 Create a culture of critical self-assessment and candid communication.

4.3.4.1 Instill a commitment to effective self-assessment throughout the security program. Encourage presentation of areas of concern before they become problems.

4.3.4.2 Create an environment in which all personnel are empowered and expected to appropriately communicate information in a clear, concise and accurate manner.

5. PROPOSED ORGANIZATIONAL STRUCTURE

The proposed organizational structure, Figure 2, separates the line function for executing the security mission from the Headquarters staff function. It establishes an operational-level organization that focuses on security implementation and standardization. Distinct roles and responsibilities are associated with tactical, operational, and strategic-level security functions. Tactical execution of contract administration occurs at the Federal field organizations. Operational implementation and standardization of operations across the security program occurs at the NA-00 level. Strategic-level policy guidance, requirements determination, and performance assessment occur in NA-70.

In order to clarify the line of authority, the CSA flows from the NNSA Administrator, through CDNS to the head of the NA-00, to the Federal field managers, and finally to the designated CSA at field sites, with no re-delegations authorized to non-Federal individuals. This authority follows the same path as the line authority from NA-00 downward. The asserted security line management tie between the Chief of Defense Nuclear Security and the security managers in the field is also terminated, in order to ensure a single, clear line of authority.

In terms of clarifying line and staff functions, the current NA-70 organization is restructured so that it serves solely as a staff organization at the strategic level. The four security offices under the current structure will be realigned into divisions with one additional division being stood up. The five divisions are Performance Assessment, Strategic Requirements (i.e., policy development, planning and requirements, and training and career development), Nuclear Materials Integration, Personnel and Facility Clearances, and Business Operations (i.e., Resource Management, Headquarters security operations, classification and controlled information, and human capital).[14]

The Performance Assessment Division is a new function responsible for assessment of contractor and Federal field organization performance, including no-notice and/or short notice assessments. This division will also evaluate training effectiveness, policy implementation, and vulnerability assessments. This is the entity that the Chief of Defense Nuclear Security would use to verify that security programs are properly implemented.

The Strategic Requirements Division is responsible for security requirement determination and the NNSA security policy process (whether that is to write new policy or interpret and amplify existing DOE policies). This division will also be responsible for establishing training requirements and developing standards and criteria for security programs. A new function of training policy and career development planning is being stood up to support Federal security professional development.

The Business Operations Division retains the existing NA-70 functions of Headquarters security operations administration and classified and controlled information. The division will be

14) The divisions of Personnel and Facility Clearances and Nuclear Materials Integration will not be addressed in this model as it does not affect the execution of the Headquarters security program function. However, an evaluation should be conducted to determine if a possible transfer of the Office of Nuclear Materials Integration is warranted.

responsible for implementation of certain activities within the NNSA security program, including the protection and control of classified information, and the physical security for NNSA Headquarters facilities and other security programs. Additionally, this division will manage the NA-70 program direction budget, establish internal controls, design and implement office protocols, and oversee records management.

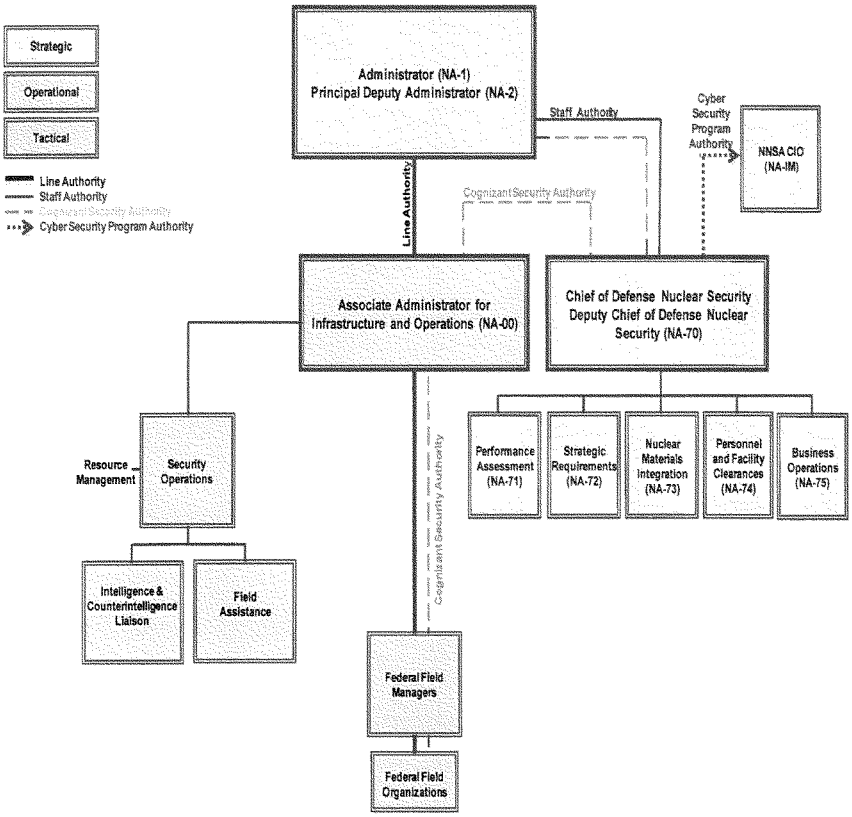
A new security operations organizational level will be stood up within the NA-00 structure. The responsibilities of this office are to ensure that the policies and guidance provided by the NA-70 staff are executed in the field. It will also ensure standardization of security procedures across the field locations as well as provide field assistance, and a conduit for field concerns to be surfaced to the NA-70 staff. It will execute the NA-70 scope and security training requirements. An expanded intelligence/counterintelligence liaison is intended to ensure that Federal security managers get needed information and have appropriate ties to law enforcement and intelligence-related agencies.

At the tactical level in the field, the multiple lines of authority are eliminated and direction will come from a single line of authority. All authorities will run through the Federal field organization manager to the appropriate security manager. The Federal field organization scope of duties will include primary contract administrative functions--including reviews of contractor reports, analysis, security plans, and other required documentation; partnering with the executing contractor; remaining knowledgeable and up-to-date on the content, operations, and effectiveness of the contractor's security implementation; alerting management of all concerns related to contractor execution of the security mission. Federal field security organizations will fulfill their contract management role.

This organizational structure will define and clarify roles and responsibilities and facilitate a strong mission focus. It divides resourcing from requirements determination in order to ensure that requirements are appropriately stated, weighed against budget resources and decisions made on accepting risks at the appropriate level. It provides a single line of authority to those operating in the field and maintains an appropriate span of control.

Figure 2

Proposed NNSA Security Organizational Structure



6. PROPOSED ASSESSMENT MODEL

The Task Force proposes a new approach to ensuring an effective security performance assessment system, one designed to address deficiencies in the current model. While retaining the three-tiered concept, it differs from the current model in several structural details and in the performance expectations established for each tier and for the system as a whole. The Task Force proposal strengthens the role of Federal security assessment within NNSA without diminishing the legitimate need for contractors to maintain their own self-assessment capabilities.

The contractor self-assessment process continues as a first tier in the overall assessment process. The primary audience for the contractor self-assessments should be the contractor security managers themselves, but the self-assessments should follow a consistent, program-wide format, and be made available for review at all higher levels of management. Contractors should be required to identify, report, and resolve security issues--sanctions should come when a higher level assessment uncovers problems that the contractor self-assessments fail to identify or properly address. Even when an issue is readily resolved and corrective actions are immediate, a finding should be issued and the corrective action recorded. Failure to do so inevitably hides potential negative trends. Contractor self-assessments should involve active performance testing rather than simply relying on work observation and document review--effective security performance can only be evaluated through testing.

The fundamental purpose of Federal security performance assessment is to ensure that requirements are properly implemented. Therefore, the primary Federal assessment organization should ultimately report to the Chief of Defense Nuclear Security, who is responsible for requirements. This provides independence not only from the contractors, but also from the tactical-level Federal field staff whose necessary day-to-day interaction with contractor managers and staff risks loss of objectivity. This enables the Chief of Defense Nuclear Security to better ensure effective implementation of NNSA security programs. Additionally, it provides feedback on performance to the operational and tactical levels.

These Federal security assessments should include performance testing of all critical elements. The assessors should issue clear findings, which are to be tracked and closed in a program-wide corrective action management system. Federal assessors should also look closely at the contractor self-assessment process; "failures to identify" by the contractor self-assessment element should automatically rise to the level of significant findings.[15]

The final tier of the assessment model should explicitly rely upon the services of an independent security oversight function, currently provided by HSS. NNSA should arrange for a regular process of comprehensive inspections. The oversight function should be encouraged to issue strong findings for matters of potential concern to the NNSA Administrator and the Secretary of

15) This model does not preclude operational and tactical level Federal managers from actively assessing contractor performance as part of their line management responsibilities.

Energy, and should routinely evaluate the performance of contractor self-assessments and the Federal assessment program.

This performance assessment model assumes a common requirements base that is employed at all levels and across the NNSA security program. While some allowance may be made for site-specific issues, the fundamental elements of this requirements base should be an appropriately integrated system of DOE policies, NNSA implementation directives, and field operational guidance. The requirements base should be reflected in approved documents such as site Safeguards and Security Plans. Specific performance requirements should be articulated in detailed performance standards and criteria supported by a commonly understood and utilized performance testing process.

7. CLOSING

Over the years, there has been tension between implementation of security and conduct of operations. Whenever there have been significant incidents of security concern, there have been corresponding swings of the pendulum towards a more rigorous security program. Security program emphasis has increased after espionage cases, internal security lapses, and external events such as the September 11, 2001 attacks. However, over time, the general trend has been for lower management levels to accept more risk in order to reduce the perceived burden and cost of the security mission. Furthermore, the trend has been to remove security from an integral mission role, adversely affecting the NNSA security program. The events at Y-12 illustrate how far the pendulum has swung in the wrong direction.

The Secretary of Energy characterized the Y-12 events as "unacceptable" and clearly stated that security is the highest organizational priority. The NNSA Administrator has been equally emphatic in numerous public statements since the incident. The evidence from Y-12 and from prior security incidents points to a culture of compromises. Moving forward, NNSA must establish and sustain an effective security program. NNSA must address the significant flaws in the current organizational structure for security and the associated assessment model. NNSA must clearly and consistently emphasize the importance of security. Ensuring that the right leadership is in the right position is absolutely critical to success. The daunting prospect--and the one that will require the consistent emphasis of current and future Secretaries of Energy and Administrators of the NNSA--will be to instill a culture that embraces security as a fundamental and essential element of the NNSA mission. If NNSA fails in this, then senior leaders will again find themselves answering to the American people for the failures of security. Sooner or later, the perpetrator will not be peacefully-minded.

APPENDICES

Appendix A

CHARTER

ASSESSMENT OF NNSA FEDERAL ORGANIZATION AND OVERSIGHT OF SECURITY OPERATIONS

1. Authorization

This Charter authorizes and directs Brigadier General Sandra Finan, United States Air Force, Principal Assistant Deputy Administrator for Military Application, National Nuclear Security Administration (NNSA), to conduct an independent critical assessment of NNSA federal organization and oversight of security operations.

2. Background

Three individuals trespassed and defaced a building at the NNSA's Y-12 National Security Complex early on July 28, 2012. As a result, NNSA is looking at all aspects of what occurred to determine both the root cause(s) of the incident and any contributing factors. This charter is focused on the path forward within the federal NNSA organization.

3. Purpose

The focus will be on the following two areas:

- Analyze current NNSA security organizational structure and recommend possible improvements that would facilitate improved operational focus, oversight, and culture sustainment.
- Analyze current NNSA security oversight model and mechanisms to determine what seams exist and what structures could be implemented to better ensure that issues are found and fixed before they become problems.

Additionally, if other areas requiring further evaluation are noted, the charter may be amended to provide additional assessment.

4. Deliverables

No later than 90 days from the date of this charter, deliver to the NNSA Administrator a report and briefing describing the analysis, findings, and recommendations. Within 45 days deliver an update with interim findings.

5. Membership

Membership will focus on individuals with a high degree of independence, expertise, and pragmatism and will be supported by NNSA. For NNSA team members, this is to be a full time detail. Team members from outside NNSA may be used to the maximum extent allowed by their host organizations.

Thomas P. D'Agostino, Administrator

8/14/2012
Date

Appendix B

Task Force Team Composition

- Brigadier General Sandra Finan, USAF*
- Mr. Roger Lewis, NNSA
- Dr. James McGee, DOE
- Lieutenant Colonel Rasheem Wright, USAF*
- Major David Coy, USA*
- Major Daniel Voorhies, USAF*

Security Liaison
Mr. Norbert Marcelle, NNSA

Technical Editor
Ms. Kimberly Hayes, Contractor

*Currently assigned to NNSA Military Element

Appendix C

Task Force Methodology

The Task Force used the following methodology in accomplishing its assignment:

1. Assembled a small group with appropriate expertise that could participate on a fully dedicated basis for the planned period of the review. This group included individuals knowledgeable and experienced in organizational analysis; security program management; security operations; performance management and performance assessment; NNSA Federal field organizations; government-owned, contractor-operated facilities; contractor performance management; M&O contracts; inspections and surveys; and human capital management and training.
2. Obtained a thorough understanding of the July 28, 2012, Y-12 security breach, initial assessments and succeeding actions. This understanding was obtained through review of draft and final reports, security video footage, briefings; and discussions with individuals, who participated in subsequent documentation and evaluation of what occurred. The Task Force focus was not on the incursion's root cause analysis or appropriate responses, but this baseline understanding was considered necessary and informative in addressing the task of analyzing the NNSA security organizational structure and the current security oversight model and mechanisms.
3. Reviewed a significant number of past reports, most notably the security assessments commonly referred to as the Chiles and Mies Reports; as well as NA-70 documents, Federal field organization documents; HSS, IG, and GAO Reports, and previously-used Standards and Criteria for evaluating DOE security program effectiveness. A selected bibliography is presented in Appendix F.
4. Reviewed written responses to a set of questions, which were answered by selected Headquarters and field organizations.
5. Conducted approximately three dozen interviews with senior Federal security managers and senior security staff (in Washington and from across the Federal field organizations) and senior contractor security representatives. This information was supplemented by discussions (not formal interviews) with others from both management and practitioner levels that the Task Force felt could be of assistance.
6. The Task Force members carefully analyzed, consistent with the terms of its charter, the information that was derived and developed. Key observations were discussed, which drove the development of findings and recommendations. After the basic conclusions and implications were formulated, the Task Force drafted this Report and reviewed the conclusions.
7. As a final quality step, before formal presentation of results to the NNSA Administrator, the "final draft" Report was further reviewed by a "Red Team" composed of experienced and qualified independent experts. The Report was finalized giving due consideration to the inputs from the Red Team.

Appendix D

Alternative Organizational Structures

The Task Force considered two additional organizational structures. While not recommended by the Task Force, the basic structural concepts are presented below.

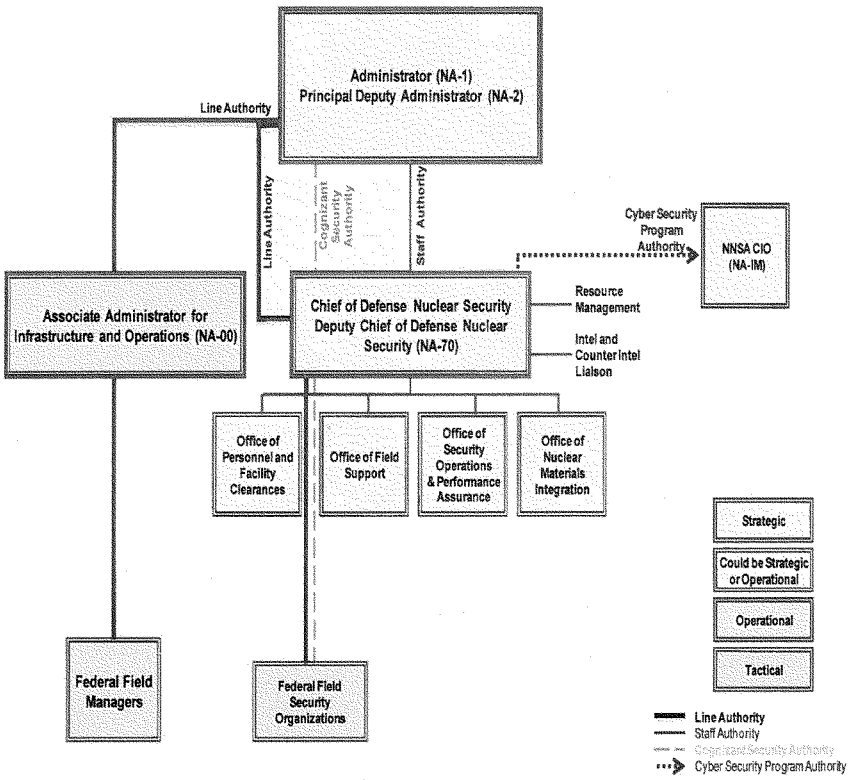
Alternative A

Centralization of the NNSA Security Function within NA-70

This structure would achieve a unified security line of authority by realigning the security organizations at each NNSA Federal field organization within Defense Nuclear Security (NA-70). At present, most senior security managers report directly to the Federal field organization manager, who provides site security guidance and direction. Currently, the Chief of Defense Nuclear Security has a dotted line to the Federal field security managers with one Specific Performance Objective into their Performance Evaluation Plan. These relationships would be fundamentally changed if the senior security managers are integrated into the NA-70 organization. The intent of this centralization option is to improve communications among Headquarters, Federal field organizations, and contractors. It could also enable NNSA to address security issues and concerns from a program-wide perspective.

Alternative A

Centralization of the NNSA Security Function within NA-70



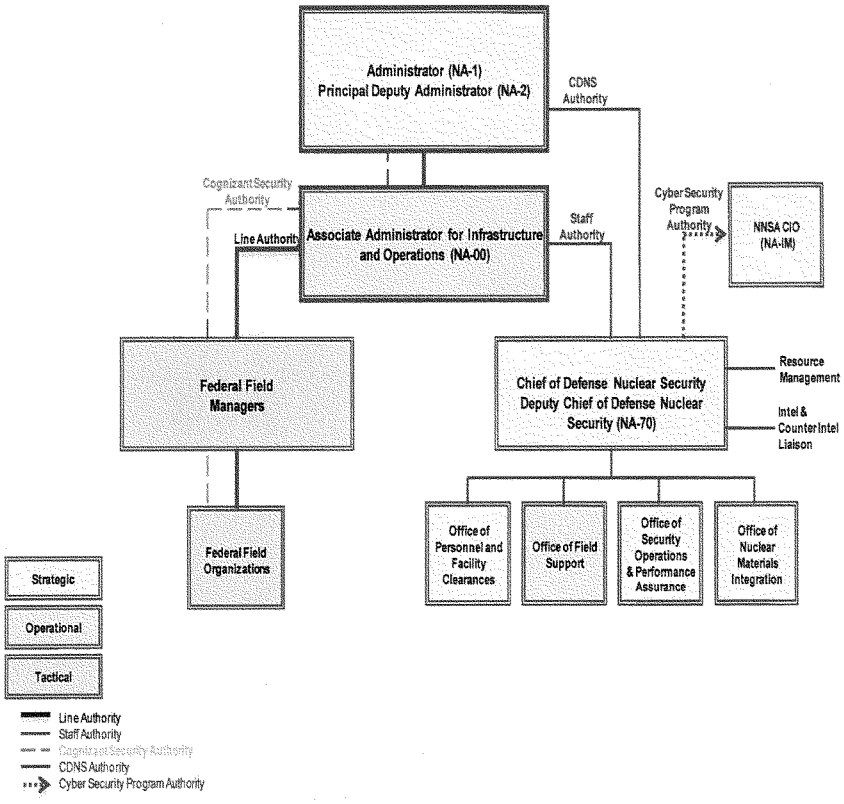
Alternative B

Centralization of the NNSA Security Function within NA-00

This structure would achieve a unified security line of authority by realigning the Office of Defense Nuclear Security directly into the Associate Administrator for Infrastructure and Operations (NA-00) organization. The statutory responsibility for the designation of the Chief Defense Nuclear Security and provision for direct access to the NNSA Administrator and the Secretary of Energy could be maintained via a separate direct communication channel. Additionally, the NA-00 would need to establish an internal organizational element focused on operational aspects of the NNSA security program. The security professionals within the Federal field organizations would have formally described relationships with both the operational element and the Office of Defense Nuclear Security while ensuring that there remains an effective communication and organizational relationship with the Federal field organizations. Current organizational relationships, including the placement of the security function in the NNSA organization, would be fundamentally changed if the Chief of Defense Nuclear Security/NA-70 is integrated into the NA-00 organization. The intent of this centralization option is to improve communications among Headquarters, Federal field organizations, and contractors. It could also enable NNSA to address security issues and concerns from a program-wide perspective.

Alternative B

Centralization of the NNSA Security Function within NA-00



Appendix E

Other Observations

In the course of its activities, the Task Force identified a variety of items that, while not rising to the level of findings in terms of the Task Force charter, were deemed worthy of inclusion in the permanent record of this review.

1. Peer reviews are not used to help ensure effective security implementation. The peer review process does not appear to be understood within the security organizations. Virtually all sites believe that an HSS assessment or an NNSA Headquarters visit constitutes adequate peer review of their operations. As a result, little data is shared between sites and the practice of evaluating security eight separate ways, without regard for how other sites operate, is perpetuated. Recommend that an effective peer review process be implemented.
2. Cyber Security responsibility as set forth in the NNSA Act is invested in the Chief of Defense Nuclear Security. Cyber Security has been delegated to NA-IM. This delegation assigns responsibility without sufficiently addressing authority and accountability. This is further complicated in that the Federal field organizations' Cyber Security function is not always integrated into the overall security program. Recommend the basis for this bifurcation be revisited.
3. A number of issues have been identified with contractor self-assessment. Critical self-assessment is not routinely accomplished and NNSA requirements are not always sufficiently tested or otherwise assessed. The current fee process as applied to security is biased toward documenting success as opposed to reality. The NNSA Acquisition Executive should evaluate options for addressing these issues in the basic contract and in the contractor performance evaluation plan.
4. There does not appear to be a correlation between issues identified and status listed in some Safeguards and Security Management Systems Assurance Program reports. In one instance, a flag was identified as "Significant Weakness" or "Unsatisfactory" performance; however, the area was identified as "Green" or "Satisfactory." Additionally, the description of the flagged item stated that "The project is and has been out of schedule". The area, however, was rated as "Green" for the first three-quarters of the year. Recommend a review of how items are reported in order to ensure the reports appropriately highlight performance.
5. The practice of using "Areas for Improvement" rather than "Findings" in assessment reports has caused follow-up actions to be weakened. "Findings" generally require a response with tracked follow-up activity. This process helps ensure that issues are appropriately corrected. "Areas for Improvement" do not require a response or follow-up. This lack of emphasis has resulted in a less stringent process to fix issues found in the assessment process and has permeated into the assessment model used by NNSA Federal staff.

6. Safeguards and Security Management Systems Assurance Program Reports are not standardized in format and content. The varied formats made analysis of the data and trend determination extremely difficult. Recommend NA-70 require all sites to submit reports in a standardized format.
7. Evaluate the role of the National Training Center (NTC) in providing professional training to the NNSA staff as part of implementing the overall recommendation for establishing an NNSA Federal security career path.
8. Consider moving the Office of Nuclear Material Integration out of NA-70. This function is not aligned well with the security mission.

Appendix F

Selected Bibliography

Public Law:

NATIONAL NUCLEAR SECURITY ADMINISTRATION ACT [As Amended Through P.L. 111–383, Enacted January 7, 2011]

DOE Orders/NAPs:

U.S. Department of Energy. Information Security. Ord. no. DOE O 471.6. June 2011.

U.S. Department of Energy. Protection Program Operations. Ord. no. DOE O 473.3. June 2011.

U.S. Department of Energy. Safeguards and Security Program. Ord. no. DOE O 470.4B. July 2011.

U.S. Department of Energy. National Nuclear Security Administration. Information Security. By Office of Defense Nuclear Security. Vol. NAP 70.4. July 2010. NNSA Policy Letter.

U.S. Department of Energy. National Nuclear Security Administration. Physical Protection. By Office of Defense Nuclear Security. Vol. NAP 70.2. July 2010. NNSA Policy Letter.

U.S. Department of Energy. National Nuclear Security Administration. Transformational Governance and Oversight. By Office of the Administrator. Vol. NAP-21. February 2012. NNSA Policy Letter.

Memorandums:

Fremont, Douglas E., Chief, Defense Nuclear Security. "Direction for Recently Issued Departmental Orders for Certain Safeguards and Security Program Areas." Memorandum. 31 Aug. 2011. MS. Washington, DC.

Poneman, Daniel B., The Deputy Secretary of Energy. "Department of Energy 2010 Safety and Security Reform Plan." Memorandum. 16 Mar. 2010. MS. Washington, DC.

D'Agostino, Thomas P., NNSA Administrator. "Six-Month Moratorium on NNSA Initiated Assessments." Memorandum to National Nuclear Security Administration. 18 Dec. 2009. MS. Washington, DC.

Abraham, Spencer, Secretary of Energy. "Delegation Order NO. 00-003.00." Memorandum to the Under Secretary For Nuclear Security. 6 Dec. 2001. MS. U.S. Department of Energy.

Badolato, E.V., Deputy Assistant Secretary for Security Affairs Defense Programs. "Direction for Safeguards and Security." Memorandum to Michael B. Seaton, DP-31. 6 Jan. 1986. MS. U.S. Department of Energy.

Internal Reports:

International Safeguards and Physical Protection. Operation Cerberus. Rep. U.S. Department of Energy, September 1986.

National Nuclear Security Administration. LOCAS Affirmation Review for the Y-12 Site Office and B&W Y-12 at the Y-12 National Security Complex. Rep. U.S. Department of Energy, June 2011.

Office of Inspector General. Management Challenges at the Department of Energy. Rep. no. DOE/IG-0858. U.S. Department of Energy, November 2011.

Office of Inspector General. Inquiry into the Security Breach at the National Nuclear Security Administration's Y-12 National Security Complex. Rep. no. DOE/IG-0868. U.S. Department of Energy, August 2012.

Office of the Inspector General. Inquiry into the Security Breach at the National Nuclear Security Administration's Y-12 National Security Complex. Rep. no. DOE/IG-0868. U.S. Department of Energy, August 2012.

Office of Defense Nuclear Security Office of Program Evaluation. NNSA Administrator's Special Focus Area # 1 Oversight of Physical Security. Rep. U.S. Department of Energy, October 2007.

Office of Health, Safety and Security. Force-on-Force Performance Tests. Rep. U.S. Department of Energy, July 2012.

Office of Health, Safety and Security. Independent Oversight Safeguards and Security Inspection of the National Nuclear Security Administration's Y-12 National Security Complex. Rep. no. OS-S-12-00100. U.S. Department of Energy, September 2012.

Secretary of Energy Advisory Board. Alternative Futures for the Department of Energy National Laboratories. Rep. U.S. Department of Energy, February 1995.

External Reports:

Baker, Howard H., Jr., and Lee H. Hamilton. Science and Security in the Service of the Nation: A Review of the Security Incident Involving Classified Hard Drives at Los Alamos National Laboratory. Rep. U.S. Department of Energy, September 2000.

Chiles, Henry G., Jr. Strengthening NNSA Security Expertise An Independent Analysis. Contract Number DE-AD26-02NT41465. U.S. Department of Energy, March 2004.

The Commission on Science and Security. Science and Security in the 21st Century: A Report for the Secretary of Energy on the Department of Energy Laboratories. Rep. 2002.

Mies, Richard W., ADM USN (Retired). NNSA Security An Independent Review. Contract Number DE-AM52-04NA99608. U.S. Department of Energy, April 2005.

A Special Investigative Panel President' Foreign Intelligence Advisory Board. Science at Its Best Security at Its Worst: A Report on Security Problems at the U.S. Department of Energy. Rep. June 1999.

United States Government Accountability Office. Modernizing The Nuclear Security Enterprise Observations on the Organization and Management of the National Nuclear Security Administration. Rep. no. GAO-12-867T. GAO, June 2012.

United States Government Accountability Office. National Nuclear Security Administration Observations on NNSA's Management and Oversight of the Nuclear Security Enterprise. Rep. no. GAO-12-473T. GAO, February 2012.

United States Government Accountability Office. Nuclear Security DOE Needs to Fully Address Issues Affecting Protective Forces' Personnel Systems. Rep. no. GAO-10-485T. GAO, March 2010.

Department of Energy
Washington, DC 20585

July 9, 2013

The Honorable Tim Murphy
Chairman
Subcommittee on Oversight and Investigations
Committee on Energy and Commerce
U. S. House of Representatives
Washington, DC 20515

Dear Mr. Chairman:

On March 13, 2013, Deputy Secretary Daniel B. Poneman, testified regarding "DOE Management and Oversight of Its Nuclear Weapons Complex: Lessons of the Y-12 Security Failure."

Enclosed are the answers to six questions that were submitted by Representatives Michael C. Burgess, Ben Ray Lujan and you to complete the hearing record.

If we can be of further assistance, please have your staff contact our Congressional Hearing Coordinator, Lillian Owen, at (202) 586-2031.

Sincerely,

Christopher E. Davis
Deputy Assistant Secretary
for Congressional Affairs
Congressional and Intergovernmental Affairs

Enclosures

cc: The Honorable Diana DeGette, Ranking Member

Printed with soy ink on recycled paper

QUESTION FROM CHAIRMAN TIM MURPHY

Q1. Please describe Department of Energy (DOE) and National Nuclear Security Administration's (NNSA) implementation plans developed in response to the recommendations provided in the Assessment of NNSA Federal Organization and Oversight of Security Operations prepared by the task force led by General Sandra E. Finan. Include in this description the specific timetables developed and funding estimates for implementing the recommendations fully.

A1. In response to the recommendations provided in the report prepared by the task force, we have focused on their observation that lines of authority and responsibility were not clearly delineated and that contractor performance was not effectively assessed. To correct those problems, we have consolidated line management authority within the Office of Infrastructure and Operations (NA-00) and refocused the Office of Defense Nuclear Security's (NA-70) mission on the development of strategic requirements and the conduct of operational security assessments. NA-70 now establishes the safeguards and security requirements and conducts field assessments to validate operational performance against those requirements. The remainder of fiscal year (FY) 2013 will be a transition period with full re-alignment and execution occurring in FY 2014.

NA-70 formed a transition team to develop and implement the realignment plan. The transition team has developed guidance in the form of a project management plan (PMP) and schedule which identifies the programs, activities, and actions necessary to support the implementation and sustainability of this organization.

The PMP activities began in February 2013 with a planned completion date of July 2014. NA-70 leadership is fully engaged in the activities and is briefed on a regular basis by the transition team lead. Ongoing communication activities are conducted to ensure NA-70 staff and NNSA leadership are kept informed of the progress as well. The increase in Federal FTEs in NA-70 will be offset by a $6M reduction in the support service contractor level of effort in NA-70.

NA-00 has developed and is implementing a subordinate Office of Security Operations (NA-00-30) to provide management and operational direction of the physical security program at NNSA facilities. Functions include management related to the protection program, physical security systems, information security, personnel security, material control and accountability, protective forces, technical security programs, and liaison with DOE's Office of Intelligence and Counterintelligence. NA-00-30 will serve as the NA-00 operational element responsible for evaluations and analyses that inform security strategies, performance objectives, and the allocation of Field Security (FS)-20 resources to meet all requirements. Consistent with the Office of Infrastructure and Operation's line management authorities, NA-00-30 will establish a self-evaluation capability aimed at ensuring the iterative improvement of NNSA security operations. In addition, NA-00-30 will participate in external reviews (e.g., DOE's Health Safety and Security, NA-70) of NNSA security operations as necessary and lead NA-00 efforts to identify security system needs, support field security activities, and share lessons learned that improve the overall security program.

NA-00 will assign program management support of the FS-20 budget activity to the Office of Infrastructure Resource Management (NA-00-50), to direct and oversee the Planning, Programming, Budgeting and Evaluation (PPBE) processes. This role includes budget formulation and programming activities regarding operational security. The proposed name change reflects the growth in scope of the office.

The security changes being effected within NNSA will require close coordination between NA-70 and NA-00 to ensure that focus is maintained on the execution of the security mission in the field while these transitions are taking place at the Headquarters. We are committed to close teamwork while establishing these new roles and responsibilities.

QUESTION FROM CHAIRMAN TIM MURPHY

Q2. Please describe DOE's plans for developing a response to the advice and observations relating to DOE's security shortcomings provided to you by Dr. Norman R. Augustine, Dr. Richard A. Meserve, and General C. Donald Alston.

A2. Following the Y-12 security breach, Secretary Chu solicited the advice and recommendations of Dr. Augustine, Dr. Meserve and General Alston to gain an informed external perspective as it related to DOE security infrastructure. The external security experts conducted a strategic review of the areas that included, but were not restricted to: contract structure, leadership, security culture, line and independent oversight strategies, and federal versus contractor security forces. The lessons learned are being applied across the DOE/NNSA enterprise and shared with the broader nuclear security community. A review of these – and other security reviews – is underway by DOE headquarters to determine whether any policy or organizational changes that should be on the enterprise-wide level.

QUESTION FROM REPRESENTATIVE MICHAEL C. BURGESS

Q1. The Secretary asked three eminent individuals to evaluate DOE culture and physical security. Their letter reports were released to the Secretary this past December, and are part of the hearing record.

Q1(a) Do you plan to produce any formal evaluation of their recommendations?

Q1(b) To their observations about security culture, what have you directed the agency to do to institute mechanisms and communications necessary to ensure a strong security culture?

A1(a) Following the Y-12 security breach, Secretary Chu solicited the advice and recommendations of Dr. Augustine, Dr. Meserve and General Alston to gain an informed external perspective as it related to DOE security infrastructure. The external security experts conducted a strategic review of the areas that included, but were not restricted to: contract structure, leadership, security culture, line and independent oversight strategies, and federal versus contractor security forces. The lessons learned are being applied across the DOE/NNSA enterprise and shared with the broader nuclear security community. A review of these – and other security reviews – is underway by DOE headquarters to determine whether any policy or organizational changes that should be on the enterprise-wide level.

A1(b) We believe that it is imperative for the Department to improve its culture so that employees feel that they can raise issues or problems to management without fear of reprisal, and know that they will be part of the process for developing effective solutions. We have found through a series of independent assessments that the Department has work to do to improve our existing culture, and this is true in both the safety and security arenas. This is a very high priority for the Department's leadership team.

QUESTION FROM REPRESENTATIVE MICHAEL C. BURGESS

Q2 In response to questioning during the hearing about terminating federal employees as a result of the Y-12 incident, you explained that disciplinary actions such as terminations are subject to due process protections. In carrying out his responsibilities, does the Secretary have sufficient statutory authority to effectuate appropriate and timely disciplinary actions relating to personnel responsible for nuclear security? And, if not, please explain what additional statutory authority may help to ensure appropriate and timely actions may be taken.

A2 With respect to initiating and effectuating disciplinary action, the Secretary has the same statutory authority afforded to heads of all other federal agencies, which is spelled out in the Civil Service Reform Act (CSRA) of 1978, Pub. L. No. 95-454, 92 Stat. 1111 (1978) (codified as amended at scattered sections of 5 U.S.C.) The current statutory scheme provides sufficient authority to effectuate appropriate and timely disciplinary actions within the Department.

QUESTION FROM REPRESENTATIVE MICHAEL C. BURGESS

Q3. According to budget data supplied to the Committee, security budgets at Y-12 carried over substantial sums from prior years that had not been expended, including approximately $55 million in fiscal Year (FY) 2011 and $36 million in FY 2012. What was communicated from National Nuclear Security Administration (NNSA) to Management and Operating (M&O) contractors or the sites to spend less than the budget authority, and what was the basis for any such directions?

A3. The Office of Defense Nuclear Security did not direct the NNSA Field Offices, or the M&O contractor, to spend less than the budget authority.

Question for Neille Miller

QUESTION FROM REPRESENTATIVE BEN RAY LUJAN

Security Funding

Q. A number of the reports observed a culture within the National Nuclear Security Administration (NNSA) of prioritizing cutting costs above the needs of security. Have Management and Operating (M&O) contractors throughout the complex been told to cut their security costs? Have security funding allocations been reduced in recent years before this incident? Has security funding been increased after the incident?

A. No, the M&O's have not been told to cut their security costs.

Security funding at some sites has been either reduced or increased depending upon operational requirements. These requirements are determined through Defense Nuclear Security's Planning Programming, Budgeting, and Evaluation (PPBE) process. The PPBE process is a formal, structured development of integrated, prioritized site security funding requirements that is validated by Defense Nuclear Security. Site security funding levels are determined based on historical cost date, current mission requirements, and any external factors that may drive funding requirements.

Following the Y-12 incident, all sites conducted assessments of their security posture, to identify any immediate funding needs for security upgrades. Some sites identified one-time costs for upgrades to specific systems. In addition, at Y-12, a shift in the protective force services from a direct contract to being provided under the M&O contractor has resulted in an increase of approximately $48 million in overhead costs applied to the Defense Nuclear

Security program. The cost model changes, however, should result in commensurate decreases to other Y-12 program customers. This cost increase associated with the contract structure change is included in outyear funding requirements at Y-12.

FRED UPTON, MICHIGAN
CHAIRMAN

HENRY A. WAXMAN, CALIFORNIA
RANKING MEMBER

ONE HUNDRED THIRTEENTH CONGRESS

Congress of the United States
House of Representatives
COMMITTEE ON ENERGY AND COMMERCE
2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6115
Majority (202) 225-2927
Minority (202) 225-3641

April 12, 2013

Major General C. Donald Alston
Retired
United States Air Force
1515 North Star Loop
Cheyenne, WY 82009

Dear General Alston,

Thank you for appearing before the Subcommittee on Oversight and Investigations on Wednesday, March 13, 2013 to testify at the hearing entitled "DOE Management and Oversight of Its Nuclear Weapons Complex: Lessons of the Y-12 Security Failure."

Pursuant to the Rules of the Committee on Energy and Commerce, the hearing record remains open for ten business days to permit Members to submit additional questions to witnesses, which are attached. The format of your responses to these questions should be as follows: (1) the name of the Member whose question you are addressing, (2) the complete text of the question you are addressing in bold, and then (3) your answer to that question in plain text.

To facilitate the printing of the hearing record, please respond to these questions by mail by the close of business on Friday, April, 26, 2013. Please also e-mail your responses to the Legislative Clerk in Word format at **Kirby.Howard@mail.house.gov**.

Thank you again for your time and effort preparing and delivering testimony before the Subcommittee.

Sincerely,

Tim Murphy

Tim Murphy
Chairman
Subcommittee on Oversight and Investigations

cc: The Honorable Diana DeGette, Ranking Member,
Subcommittee on Oversight and Investigations

Attachments

QFRs submitted by the Honorable Ben Ray Lujan
Subcommittee on Energy and Commerce
DOE Management and Oversight of its Nuclear Weapons Complex:
Lessons of the Y-12 Security Failure

1. **I have some questions related to Mr. Augustine's report that I hope the two of you might address given that his report was entered as part of your testimony and that your own investigations may have led you to have some opinions on these topics. Mr. Augustine wrote that "What is needed is not more inspections but better inspections." And that "Site office responsibility is not to manage work but to assure that work is managed." And finally that "headquarters personnel should not seek to involve themselves in the actual execution of routine work, but should use their full authority to ensure the significant work is in fact properly executed." It seems to me Mr. Augustine was concerned about different levels of oversight not having clearly defined roles. Did you see evidence for this and do you agree that what is needed is not more oversight but more effective oversight?**

   We are not in a position to speak for Mr. Augustine, but we concur in your interpretation of the thrust of Mr. Augustine's letter. We agree that an improvement of the inspection process is appropriate and that the differing responsibilities of the site offices and the headquarters need to be clearly defined. We also urge that the security capabilities of both the headquarters and field offices should be upgraded and that both offices should complement each other's activities.

2. **Not all aspects of what was found at Y-12 will generalize and be applicable to all NNSA sites. In particular, production facilities are very different from the design and engineering labs. Which of the lessons from Y-12 in your opinion are readily generalized across all sites and which ones will require adjustment to meet the unique aspects or mission needs of each lab?**

   The focus of our inquiry was on the structure for the management of security. We believe that our suggestions for clarification of authority and responsibility, for the encouragement of an appropriate security culture, and for improvement of federal oversight are widely applicable across the weapons complex. The details of the security plan may well be very different from site to site in light of the varying circumstances (e.g., geography, defensive strategy), the different types of work that are conducted, the different masses and types of materials, different vulnerabilities, and the like.

FRED UPTON, MICHIGAN
CHAIRMAN

HENRY A. WAXMAN, CALIFORNIA
RANKING MEMBER

ONE HUNDRED THIRTEENTH CONGRESS

Congress of the United States
House of Representatives
COMMITTEE ON ENERGY AND COMMERCE
2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-6115
Majority (202) 225-2927
Minority (202) 225-3641

April 12, 2013

Mr. David C. Trimble
Director
U.S. Government Accountability Office
441 G Street, N.W.
Washington, D.C. 20548

Dear Director Trimble,

Thank you for appearing before the Subcommittee on Oversight and Investigations on Wednesday, March 13, 2013 to testify at the hearing entitled "DOE Management and Oversight of Its Nuclear Weapons Complex: Lessons of the Y-12 Security Failure."

Pursuant to the Rules of the Committee on Energy and Commerce, the hearing record remains open for ten business days to permit Members to submit additional questions to witnesses, which are attached. The format of your responses to these questions should be as follows: (1) the name of the Member whose question you are addressing, (2) the complete text of the question you are addressing in bold, and then (3) your answer to that question in plain text.

To facilitate the printing of the hearing record, please respond to these questions by mail by the close of business on Friday, April, 26, 2013. Please also e-mail your responses to the Legislative Clerk in Word format at **Kirby.Howard@mail.house.gov**.

Thank you again for your time and effort preparing and delivering testimony before the Subcommittee.

Sincerely,

Tim Murphy

Tim Murphy
Chairman
Subcommittee on Oversight and Investigations

cc: The Honorable Diana DeGette, Ranking Member,
Subcommittee on Oversight and Investigations

Attachment

Additional Questions for the Record, House Committee
on Energy and Commerce, Oversight and Investigations Subcommittee, Chairman Murphy

The Honorable Tim Murphy

1. *In its September 12 testimony, GAO credited NNSA with having an effective headquarters security organization that had been able to conduct security reviews, develop security performance measures and institute a security lessons-learned center. Can you explain why and how your view has changed?* **We noted progress between our 2003 and 2007 reviews of NNSA's headquarters security organization. For example, our May 2003 report found that NNSA had not been fully effective in managing its safeguards and security program in a number of areas including defining roles and responsibilities and allocating staff.[1] In January 2007, although we noted some similar weaknesses, we also found that NNSA had begun to build an effective security organization.[2] Between 2007 and 2012 we continued, through recommendation follow-up and other interactions, to witness positive trends in the management of NNSA security. These views are reflected in our September 2012 testimony.[3] As our March 2013 testimony notes, however, some of the reviews conducted in the wake of the Y-12 incident uncovered negative and apparently unresolved aspects of NNSA's security organization such as confused lines of authority and lack of site assessment capability.[4] NNSA recently announced plans to address these problems and we plan to examine them closely in our ongoing review of NNSA security reform for the Subcommittee. This review will be complete later this year.**

---

[1] Government Accountability Office (GAO), *Nuclear Security: NNSA Needs to Better Manage Its Safeguards and Security Program*, GAO-03-471 (Washington, D.C.: May 30, 2003)
[2] GAO, *National Nuclear Security Administration: Additional Actions Needed to Improve Management of the Nation's Nuclear Programs*, GAO-07-36 (Washington, D.C.: Jan.19, 2007).
[3] GAO, *Modernizing the Nuclear Security Enterprise: Observations on the National Nuclear Security Administration's Oversight of Safety, Security, and Project Management*, GAO-12-912T (Washington, D.C.: Sept. 12, 2012).
[4] GAO, *Modernizing the Nuclear Security Enterprise: Observations on DOE's and NNSA's Efforts to Enhance Oversight of Security, Safety, and Project and Contract Management*, GAO-13-482T (Washington, D.C.: Mar. 13, 2013).

2. *In response to other witness testimony, would federalizing NNSA security organization, to include security forces, change the agency's security culture?* **We generally agree with the findings of the Secretary of Energy's 2012 panel which found, among other things, that NNSA needed to improve its security culture. The members of the panel believed that federalization could serve as a catalyst for cultural change. While this is possible, our January 2010 report on DOE and NNSA protective forces found that federalization of these forces may be difficult to implement.[5] For example, current contractor protective forces might face a loss of pay or even a loss of their jobs as these forces would have to compete with other applicants for the newly created federal jobs. In addition, according to Office of Personnel Management officials, federal retirement benefits would not be granted, under existing laws, for previous years of contractor service. Nevertheless, if DOE and NNSA cannot enact cultural change themselves, far-reaching and fundamental reforms such as federalization may need to be considered.**

3. *How did DOE respond to your GAO work on its safety reform efforts?* **We made a number of recommendations in our April 2012 report on safety reform.[6] In February 2013, DOE reported to us that it is developing action plans or tracking mechanisms in response to our recommendations. Specifically:**

   - ***GAO Recommendation: Provide DOE sites and contractors with a plan on implementing the Safety Reform effort that includes results-oriented outcome measures.*** **DOE reports that it is developing a comprehensive training matrix for all new directives and requirements, and is monitoring the implementation of all new directives.**

---

[5] GAO, *Nuclear Security: DOE Needs to Address Protective Forces' Personnel System Issues*, GAO-10-275 (Washington, D.C.: January 29, 2010).
[6] *GAO, Nuclear Safety: DOE Needs to Determine the Costs and Benefits of Its Safety Reform Effort*, GAO-12-347 (Washington, D.C.: April 20, 2012).

- ***GAO Recommendation: Ensure that the plan developed for sites and contractors details how the reform effort (revised directives) will help address past safety problems.*** **DOE reports that it: (1) has developed a report that details activities and plans for implementing effective quality assurance requirements; (2) is developing a plan to identify activities for effective implementation of Safety Management; and, (3) is developing a plan to identify activities for implementing effective federal oversight.**

- ***GAO Recommendation: Clearly define and implement independent oversight roles.*** **DOE reports that HSS is developing a memo for the Secretary to re-affirm the Department's commitment to independent oversight of safety and security.**

We are currently monitoring DOE's implementation of these activities.

○