Statement before the U.S. House of Representatives
Committee on Armed Services
Subcommittee on Strategic Forces

Hearing on

Nuclear Security:

Actions, Accountability, and Reform

A Statement by

C. Donald Alston

Major General, USAF (retired)

February 28, 2013

Rayburn House Office Building Room 2212

Nuclear Security:
Actions, Accountability, and Reform

Statement of C. Donald Alston
Major General, United States Air Force (retired)
Before the Subcommittee on Strategic Forces
of the U.S. House of Representatives Committee on Armed Services

February 28, 2013

Mr. Chairman, Ranking Member Cooper, members of the subcommittee, I thank you for the opportunity to appear before you today as part of this distinguished panel.

With the subcommittee's permission, I would like to submit as my statement three separate letters, authored by Mr. Norman Augustine, Dr. Richard Meserve, and me, which we provided to Secretary of Energy Dr. Stephen Chu in support of our examination of physical security at Department of Energy Category 1 nuclear facilities. In October 2012, Secretary Chu asked the three of us to consider a variety of security models and to provide our separate, individual observations regarding any emerging constructs that may be viable 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.

I would also like to provide some additional context about our assessments for the purpose of clarity. While Secretary Chu did not ask us to investigate the Y12 security breach in particular, we used that incident and resulting investigations as an entry point into a larger examination of the physical security construct. 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.

Mr. Chairman, Ranking Member Cooper, and members of the subcommittee, below are letters to Secretary Chu from my esteemed colleagues and me. Thank you for the opportunity to appear today before the subcommittee, and I 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

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

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.

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.

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

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.

- 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 Phone
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