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.