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