Safeguarding Nuclear Waste – A Study in Risk Management and Overcoming Significant Challenges-16439

By
Dr. Gerald D. Curry, DOE/EM-44

ABSTRACT

Three years after what is commonly referred to as the "Y-12 Incident", where three individuals trespassed and defaced a building at the Department of Energy's (DOE) Y-12 National Security Complex early on July 28, 2012, the DOE commissioned study after study to review security practices and internal risk management safeguarding protocols that preserves safety and a secure environment. These studies highlighted systemic organizational dysfunctions, critical leadership shortcomings, and communications failures. Much attention has been focused on risk management and security oversight practices. This analysis presents an update on the Department's Environmental Management (EM)-wide security leadership improvements designed to restore public confidence and explain how a deeper risk analysis has elevated security oversight into a common-core Department of Energy achievement. While EM is not the managing Program Office for Y-12, this event had a DOE-corporate wide impact.

I. INTRODUCTION

When the perimeter was breached at Y-12, in July 2012, it caused epic security scrutiny by security experts throughout the national nuclear security enterprise. National industry leaders were summoned to offer opinions and recommend how to repair security within the Department. Several studies were conducted to identify root cause solutions, and make suggestions to right-steer or even completely overhaul security if required.

Results of these studies identified four central themes fostering poor security execution in the field: 1) lack of policy transparency, 2) excessive bureaucracy, 3) haphazard accountability, and 4) confusing policies. The purpose of this paper is to leverage the wisdom contained in the various reports and case studies, and by highlighting the significant success across the Department of Energy, specifically within the Environmental Management Safeguards and Security Office, more commonly referred to as EM-44. Secondly, to restore public confidence in the

Department's leadership by highlighting industry benchmark strategies resulting in significant enduring improvements.

This paper takes a critical review into the legacy security problems and challenges that plagued the Department, many of which were mentioned in the various investigative reports and case studies, while some of the data used in building this paper came from personal interviews from employees who lived through the Y-12 Incident, and continue to support the Department. All information gathered for this paper is authentic and received freely from each participant.

Several historical reports, memorandums, and studies were used in formulating this response has shaped the security landscape strategies, behaviors, and mindsets for the past few years. Understanding the concept of *Risk* is critically important in this paper; how risk is applied, which risk is acceptable, and when risk should be mitigated is addressed. Several security systems were explored and policies investigated to accurately reflect on the improvements within EM-44 for the past three years.

II. REFLECTIONS ON Y-12 INCIDENT

The safety, security and safeguards of facilities storing and processing nuclear material is an important national concern. The incident at Y-12 was an anomaly, inconsistent with the professional level of security found at all Department sites. The protective service, supporting contractor staff, and federal employees charged with the full spectrum of security oversight endure hours of security training to ensure trespassing opportunities never occur. Security is everyone's business, and the entire workforce contributes to maintaining a safe and secure environment.

During the early morning hours on July, 28, 2012, three protestors crossed several security boundaries and vandalized the exterior wall of a facility holding significant quantities of highly enriched uranium (HEU). The HEU was still several additional protective layers from the protestors, and was never within immediate access to the three violators. The National Nuclear Security Agency (NNSA) confirms security at various levels did not function that day in the way it was designed for various reasons. The purpose of this paper is not to deliberate why certain security systems did not perform correctly, but to focus on the breakthrough improvements EM-44 has made since this event. Executing security is a collaborative endeavor and requires all elements within the Department to work together in an affirming way.

The Y-12 incident received industry-wide notoriety for all the wrong reasons, but if there is a silver lining, it must be the increased attention from senior DOE and

government leader's singular focused on improving security. As previously mentioned, the Department commissioned several studies be conducted to better understand the basic concepts of security operations, and the health and status of security nationwide. One of the first studies to be requested, was by former U. S. Nuclear Regulatory Commission Chairman, Richard A. Meserve, now serving as ninth President of Carnegie Institution for Science. In his letter to then Secretary Steven Chu, he identifies a fractured management structure and calls for aligning of authority and responsibility. Meserve highlights the poor interface between federal officials and contractors as *"just not working"*.

The Merserve Report, or more commonly termed the "Secretary Chu Report", asks for improved federal oversight, detailing security systems not functioning properly and federal officials not following up to improve security system operations. Merserve recommends enhancing the protective force, by inventing a security culture based on transparency steeped in security operations. Merserve concludes by emphasizing the need to balance security posturing by integrating physical, cyber, and personnel security to reduce aggregate vulnerabilities.

The second study was conducted by Norman R. Augustine, retired chairman and chief executive officer for Lockheed Martin Corporation, the nation's largest defense contractor and former Under-Secretary of the Army. Augustine concludes a culture of accommodation and passiveness when in the presence of subpar performance was deeply entrenched within the DOE culture. He added *"a culture of tolerance overcame a culture of performance".* Augustine details several recommendations within his report that senior leaders should consider for facilitating sustained security improvements.

The third report on the Y-12 Incident is from C. Donald Alston, retired U. S. Air Force Major General, and Strategic Deterrence and Nuclear Integration Commander, and U.S. Air Force Assistant Chief of Staff, observed, *"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"*. He continues, *"A pervasive culture in which each member of the nation's nuclear weapons complex recognizes the vital role he/she plays in ensuring both security and safety contributes directly to maintaining that credibility."* The Alston report fashions the horrent results of this incident around leadership, and its inability to communicate effectively is the collective responsibility of the entire workforce.

In the backdrop of these three reports, more commonly referenced within the Department as the "Three Wise Men Letter Reports", ten previous reports solely focusing on security had been commissioned by the Department dating back as far as 1986 (See Reference Section). Collectively, millions of dollars were spent, sage

and prudent advice presented, yet the same significant security challenges continued for years perhaps because the Department did not fully understand how to develop, monitor, and implement these recommendations. This paper will show how some of these previous reports are being considered to move security in a more effective and productive environment.

The final and most recent report was conducted by U.S. Air Force Brigadier General Sandra Finan, Global Strike Command, Commander, who led a team consisting of NNSA, DOE, and military specialists who were charged with examining the NNSA security organization structure, and security oversight model being used throughout the agency. General Finan concludes, *"This lack of clear lines of authority contributes to a widespread practice of decision-making by consensus. When consensus fails, organizational elements can act independently or not at all, which undermines effective implementation of the security program."* This report crystalizes the point by confirming*, "Ensuring that the right leadership is in the right position is absolutely critical to success."* She draws a direct linkage between sound security principles and strong leadership.

In essence these reports cite leadership as the dominant factor required for creating a successful security culture in any organization. Each of the studies centered leadership as the single common shortcoming. Security leadership should be competent in the full spectrum of security, and equipped with the authority to make significant decisions unabated from narrow-minded traditional processes not grounded in reasonable risk management principles. New security leadership should be fastened with uncompromising integrity, while processing a professional record of nurturing teams successfully. At the Department-level, security lines of authority would be enhanced if security was commanded by a single appointee, and not divided among competing components struggling with overlapping roles and responsibilities, and budgetary limitations.

III. WHAT WE ARE DOING?

Completely ignoring the recommendations from these studies would be irresponsible. In the pursuit for answers, the Department mandated close examination of the various security organizations to identify synergies, duplications, and overlaps in policy development and execution. In February 2014, the Deputy Secretary directed the formation of the Chief Security Officers (CSO), established with senior security representatives from each of the three Under Secretarial organizations: Environmental Management, Science, and NNSA. This senior level group provides security oversight and synergy for the Department. The CSO forum is chaired by Chief of Staff for the Deputy Secretary.

The CSOs have three primary functions: develop recommendations regarding Department-wide security policies, facilitate active coordination of effective security strategies across the Department, and provide a forum for addressing cross-organizational issues and challenges. The CSOs sponsored a collaborative effort to determine the status of security at Category I and Category II facilities based on; vulnerability and risk assessments, performance testing data, and internal and external independent assessments. These assessments are conducted on DOE policy timelines and include independent Headquarters Inspections, Extent of Condition Reviews, Program Office Assessments, Field Office Surveys, and Contractor Self-Assessments.

This CSO forum meets bi-weekly to discuss emerging threats to DOE mission areas, identify potential collaborative initiatives and innovative opportunities where all organizations can benefit. When mission failures are identified, quick resolutions are sought from across the entire DOE community to help foster unity and pride. Security is a team activity and the CSO forum ensures the entire community is informed and aware of security requirements.

IV. EM-44 ORGANIZATION

The EM mission is designed to address the nation's Cold War environmental legacy resulting from five decades of nuclear weapons production and many more decades of government-sponsored nuclear energy research. This legacy includes some of the world's most dangerous radioactive sites with large amounts of radioactive wastes, spent nuclear fuel (SNF), excess plutonium and uranium, thousands of contaminated facilities, and contaminated soil and groundwater. Established in 1989, the EM office has cleaned up 90 of the original 107 sites assigned. The EM office continues its responsibility of cleaning up legacy waste remaining from nuclear material from the Cold War era.

The EM-44 mission is to oversee the implementation of policy and guidance with respect to security and emergency management, by fostering continuous improvement across the EM complex through application of Integrated Safeguards and Security Management principles. The EM-44 directorate performs its critical mission with a modest thirteen federal employees, and five contractors, who are assigned various task that support the mission. These eighteen people perform the work of twice as many.

The EM-44 organization is led by Jimmy McMillian, a retired U.S. Air Force Brigadier General, and serves as the Chief Security Officer for DOE Headquarters, and Environmental Management (EM). He reports directly to the Associate Deputy Assistant Secretary for Safety, Security, and Quality Programs for Environmental Management (EM-40), who reports to the Assistant Secretary for Environmental Management (EM-1). EM-44 has two primary functions: Safeguards and Security oversight (Protection Program Management, Physical, Protective Force, Personnel, Information, Material Control and Accountability), Emergency Preparedness oversight at all EM sites from Category I to IV.

EM-44's primary focus is obtaining and sustaining audit readiness for all assigned programs, and ensuring undeniable accountability for every security function charged to the Directorate. Since September 2013, the Director has visited each site multiple times each year, improving EM-44's rapport with the entire workforce. The primary goal of these visits is meeting people actually conducting the tactical critical tasks, building trust and transparency with federal contractor staff.. Moreover, EM-44 focuses on identifying issues with potential for interfering with mission goals and collaborates with site leadership to find permanent solutions. Desk Officers are required to visit their sites to connect with federal and contracting staffs, who conduct daily security duties and identify issues with potential to affect operational readiness.

EM-44 requested each branch of his office (Security, Classification, and Emergency Preparedness) conducts Vulnerability Assessments, and Surveys to evaluate operational readiness status of the site preparing for a Department-level assessment. These assessments provides the site opportunities to closely examine internal security protocols, and test Headquarters directives in real-time scenarios, and serves as a benchmark for Headquarters Enterprise Assessment Evaluations. The feedback from each site has been overwhelmingly positive and serves as another data point in delivering audit readiness.

To strengthen the communications with the sites, EM-44 hosts a quarterly video teleconference (VTC) with EM sites collectively. This forum is interactive and gives the site security teams the platform to surface their concerns for quick resolution. Weekly, EM staff meetings are held and solely site-centric. Each desk officer highlights the site's highest priorities, operational issues, critical decisions requiring attention, and future events demanding attention. These meetings are typically held for approximately one to one and a half hours. In March 2014, EM-44 hosted its first Summit where they took time out to wrestle with their internal challenges, and establish meaningful goals that set the agenda for the following year. This event was held again, in March 2015, to measure all progress since the previous event, and tweak current strategic goals.

EM-44 is developing security trends to share with the sites to improve security standards. In August 2015, quarterly metrics are being collected to identify duplications, overlaps, shortages, and disconnects. Very rarely in the future, will EM-44 have to request routine information from the site, because critical mission information is being organically warehoused internally. Naturally, it will take some time to gather depth in these mission-centric databases, but over time this information will be leveraged and made available to each desk officers to quickly resolve operational needs.

In an effort to improve the culture within EM-44, each employee is encouraged to enrolled in leadership courses, and complete the next academic degree if desired. Each employee is given the opportunity to share their personal concerns daily, in an environment without judgement. Mr. McMillian maintains an open-door policy where every employee can enter and share their thoughts and concerns.

V. RISK MANAGEMENT

To help bolster common, interoperable, and systematic approaches to risk management, EM-44 has employed a standardized risk management process. This approach promotes comparability and a shared understanding of information and analysis in the decision process, and facilitates better structured and informed decision making.

This risk management process adopted by EM-44 consist of;

- Defining and framing decisions in the context of goals and objectives
- Identifying the risks associated with the goals and objectives
- Analyzing and assessing the identified risks
- Developing alternative actions for managing the risks and creating opportunities, and analyzing the costs and benefits of those alternatives
- Making a decision among alternatives and implementing that decision, and
- Monitoring the implemented decision and comparing observed and expected outcomes to influence subsequent risk management alternatives and decisions.

Understanding and operating risk management principles are fundamental in making security decisions. Risk analysis concepts establish the doctrinal underpinnings for institutionalizing a risk management culture through consistent application and training on risk management principles. Since the Y-12 incident, one of EM-44's primary responsibilities has been to promote a common understanding of and a standard approach to risk management. Risk Management in EM-44 consist of safeguarding special nuclear material (SNM), material control

and accountability (MC&A), industrial (badging, facility access), classification (information/document protection programs) security, emergency preparedness, which includes Continuity of Operations Planning (COOP) is all a part of the full spectrum of security operations.

EM-44 is directly responsible for conducting Protective Force Capability Assessments, and within the execution of this duty, risk management allows planners to prioritize which capabilities have the greatest return on investment in preparedness activities. Risk management can also help identify which capabilities are most relevant to an organization and identify potential capability gaps. The practice of risk management allows for a systematic and comprehensive approach to security decision making. Risk management promotes the development and use of risk analysis to inform the selection of alternative strategies and actions and to evaluate the effectiveness of the required activities.

Standard risk management principles are not designed to promote uniformity or conformity; rather, they offer broad guidance that should be uniquely tailored for the specific needs of each organization. While a “one-size-fits-all” approach for security operations, or risk management is neither feasible nor desirable. All DOE risk management programs should be based on 1) enhancing the overall decision making process, and 2) is used to control and shape risk, but cannot eliminate all risk.

In light of the Y-12 incident, EM-44 quickly realized when communicating risk to the site, it was important to consider the intended audience and tailor the language and channels used to effectively convey the information to promote and elicit the desired action and outcomes. To be both clear and transparent was extremely important to communicate in a direct, simple and understandable way. Transparency in communications means disclosing assumptions, methodology, and uncertainty being considered. This direct method of communications has paid dividends within the EM-44 staff and while servicing the sites.

Communication efforts with decision makers and industry stakeholders have been proactive and a critical part of the risk management process. Risk information is readily available for relevant parties at all stages of the risk management cycle. This style of communications creates trust. EM-44 has learned that consistency is important, and untenable in light of emerging information, then officials need to acknowledge it, including any errors that may be involved, and explain it. Once trust is lost, it is very difficult to recover.

EM-44 confirms that communications connects each step of the risk management process. It is crucial for linking the risk management principles and process. One cannot overstate the importance of risk communications in risk management.

VI. EPILOUGE

Managing security of SNM is a critical mission and one that is taken seriously by everyone involved in the process. The Y-12 Incident shined a bright light on how security was being executed within DOE to the entire world. The reports from the Y-12 Incident all confirm leadership was a significant problem prior to this event, but since that time EM has made tremendous strides by refocusing positive attention where it is needed. Through principles of strong leadership involvement, professional engagement, and adherence to a risk management processes, EM-44 is turning the tide in a positive direction by building trust at all levels, holding stakeholders accountable, and creating depth in every layer of security system support.

EM-44 is rapidly reaching its goal of being audit ready by remaining relevant and actively involved at each site. Improved security vulnerability assessments are being conducted at each site, capabilities planning is occurring for each Protective Force team, MC&A, and classification records are being scrutinized, with feedback being delivered to the sites, to enhance accountability. Collectively all these actions are building a trusting relationship fostered around professional competence and caring. There is a saying, "…no one cares about a leader, until they know how much that leader cares." The new EM-44 has demonstrated how much he cares by instituting local policies and practices that positively impact the entire security community.

The security leadership across DOE is stronger, more alert, and prepared for adversity of any sort. Creating the CSO Committee has expedited response time, quickened coordination, and united expertise when needed. The entire DOE security leadership apparatus is properly poised for emerging threats in a rapidly changing environment. When reflecting on the aftermath of the Y-12 Incident the margins of improvements are wide and deep. DOE has leveraged this unfortunate incident by closely examining all aspects of security and installing the necessary protocols required in carrying out their important mission.

DEFINITIONS

Appraisal: An appraisal is an Independent Oversight activity conducted by the Office of Enterprise Assessments to evaluate the effectiveness of line management performance and risk management or the adequacy of DOE policies and requirements.

Best Practice: A best practice is a safety or security-related practice, technique, process, or program attribute observed during an appraisal that may merit consideration by other DOE and contractor organizations for implementation because it: (1) has been demonstrated to substantially improve safety or security performance of a DOE operation; (2) represents or contributes to superior performance (beyond compliance); (3) solves a problem or reduces the risk of a condition or practice that affects multiple DOE sites or programs; or (4) provides an innovative approach or method to improve effectiveness or efficiency.

Benchmarking: Benchmarking improves performance by identifying and applying best demonstrated practices to operations and sales. Managers compare the performance of their products or processes externally with those of competitors and best-in-class companies and internally with other operations within their own firms that perform similar activities. The objective of Benchmarking is to find examples of superior performance and to understand the processes and practices driving that performance.

Institutional Risks: Risk associated with an organization's ability to develop and maintain effective management practices, control systems, and flexibility and adaptability to meet organizational requirements.

Line Management: Line management refers the unbroken chain of responsibility that extends from the Secretary of Energy to the Deputy Secretary, to the Secretarial Officers who set program policy and plans and develop assigned programs, to the program and Field Element Managers, and to the contractors and subcontractors who are responsible for execution of these programs. It is distinct from DOE support organizations, such as the Office of Environment, Health, Safety and Security, Office of Management, and Office of the Chief Information Officer, which also have responsibilities and functions important to security and safety.

Major Vulnerability: A vulnerability which, if detected and exploited, could reasonably be expected to result in a successful attack causing serious damage to the national security.

Operational Risks: Risk that has the potential to impede the successful execution of operations with existing resources, capabilities, and strategies.

Opportunities for Improvement: Opportunities for improvement are suggestions offered in Independent Oversight appraisal reports that may assist cognizant managers in improving programs and operations. While they may identify potential solutions to findings and deficiencies identified in appraisal reports, they may also address other conditions observed during the appraisal process. Opportunities for improvement are provided only as recommendations for line management consideration; they do not require formal resolution by management through a corrective action process.

Performance Testing: Activities conducted to evaluate all or selected portions of safety and security systems, networks, or programs as they exist at the time of the test. Performance testing includes, but is not limited to, force-on-force exercises, tabletop exercises, knowledge tests, limited-scope performance tests, limited-notice performance tests, penetration testing, vulnerability scanning, continuous automated scanning, and cyber security "red teaming." Performance testing can be conducted as part of a scheduled appraisal activity (i.e., announced), or without prior knowledge of the entity being tested (i.e., unannounced).

Policy: The term "DOE policy" or "policy" when used in lower case in this Order is meant to be all inclusive of documents describing the philosophies, fundamental values, administration, requirements, and expectations for operation of the Department. It includes but is not limited to DOE Policies and other types of directives issued under DOE O 251.1.

Recommendations: Recommendations are suggestions for senior line management's consideration for improving program or management effectiveness. Recommendations transcend the specifics associated with findings, deficiencies, or opportunities for improvement and are derived from the aggregate consideration of the results of the appraisal.

Strategic Risks: Risk that affects an organization's vital interests or execution of a chosen strategy, whether imposed by external threats or arising from flawed or poorly implemented strategy.

REFERENCES

Report Title: C. Donald Alston letter to Secretary of Energy Steven Chu
Report Date: December 6, 2012
Scope: Professional assessment of security breach at the Y-12 National Security Complex
Summary: DOE/NNSA-wide assessment of security

Report Title: Norman R. Augustine letter to Secretary of Energy Steven Chu
Report Date: December 6, 2012
Scope: Professional assessment of security breach at the Y-12 National Security Complex
Summary: DOE/NNSA-wide assessment of security

Report Title: Richard A. Meserve letter to Secretary of Energy Steven Chu
Report Date: December 6, 2012
Scope: Professional assessment of security breach at the Y-12 National Security Complex
Summary: DOE/NNSA-wide assessment of security

Report Title: Assessment of NNSA Federal Organization and Oversight of Security Operations, Sandra E. Finan, BRIG GEN, USAF
Report Date: November 7, 2012
Scope: DOE/NNSA-wide assessment of security
Summary: Transmittal of Task Force Report on the Assessment of NNSA Federal Organization and Oversight of Security Operations

Report Title: Federal Advisory Committee for the Nuclear Command and Control System Comprehensive Review (Admiral Mies Report)
Report Date: December 3, 2009
Scope: Comprehensive review of the implementation of National Security Presidential Directive 28.
Summary: Cultural, personnel, organizational, policy, and procedural issues exist because of a lack of clear accountability, excessive bureaucracy, organizational stovepipes, lack of collaboration, and unwieldy, cumbersome processes. Recommendations are that NNSA work within DOE to develop a more robust integrated DOE/NNSA-wide process to provide accountability and follow-up on security finding and recommendations. Further supports the findings of the Chiles report.

Report Title: Strengthening NNSA Security Expertise, an Independent Analysis (Chiles Report)

Report Date: March 2004
Scope: Post 9/11 look at long-term management of the NNSA security program.
Summary: The Report identified organizational weaknesses in the areas of human capital management, security information flow, and the NNSA S&S strategic plan. The recommendations included improving the training, qualifications and stature of the NNSA security workforce, instituting security staff rotation, identifying options for accelerating the security clearance process, improving security information flow, revising the NNSA safeguards and security strategic plan, and providing budget support for these recommendations.

Report Title: Science and Security in the Twenty First Century: A Report for the Secretary of Energy on the Department of Energy Laboratories (Hamre Report)
Report Date: February 2002
Scope: Integration of security and science at DOE laboratories.
Summary: The Commission's overarching finding was that DOE's policies and practices risk undermining its security and compromising its science and technology programs. The following five recommendations were provided to address this finding: clarify lines of responsibility and authority; integrate science and security; develop and practice risk-based security; adopt new physical security tools and analytical techniques; and strengthen cyber security.

Report Title: Science and Security in the Service of the Nation: A Review of the Security (Baker/Hamilton Report)
Report Date: September 2000
Scope: Independent review of the underlying causes and what happened regarding the lost hard drive at the Los Alamos National Laboratory.
Summary: The review team stated that there was confusion over the respective S&S oversight roles and responsibilities, the report specifically stated: " line management for security, in the area of oversight there has existed a confusion of responsibilities, as there are two offices let by senior DOE officials with apparent oversight responsibilities and authorities."

Report Title: Science at Its Best, Security at Its Worst (Rudman Report)
Report Date: June 1999
Scope: President directed the President's Foreign Intelligence Board (PFIB) to review of the structural and management problems with the DOE security program.
Summary: The report concludes that DOE is incapable of reforming itself to address known security program problems. The PFIB also found that the weapons laboratories have a deeply rooted culture of low regard for and, at times, hostility to security issues, which has continually frustrated the efforts of its internal and external critics, notably the GAO and the House Energy and Commerce Committee. In light of this conclusion, the primary recommendation to address this conclusion

is to divest DOE of the management of the weapons research and stockpile programs and to establish a new semi-autonomous agency within DOE that has the clear mission, streamlined bureaucracy, and drastically simplified lines of authority and accountability. The PFIB believed that this action would insulate the weapons laboratories from many of DOE's historical problems and promote the building of a responsible culture over time.

Report Title: Alternative Futures for the Department of Energy National Laboratories (Galvin Report)
Report Date: February 1995
Scope: Prepared by the Secretary of Energy Advisory Board to provide alternate futures for DOE laboratories and to propose alternatives for directing resources at the labs toward the economic, environmental, defense, scientific, and energy needs of the nation.
Summary: The overall finding is that the Department has excessive oversight and is micromanaging the laboratories. The report concludes that the Department and Congress should manage as a "private sector style-corporatized- laboratory system" (Performance-based oversights, regulated by industry standards, consolidate or eliminate DOE field offices, and apply business budgetary principles).

Report Title: Management Survey and Analysis, Office of Intelligence and National Security, Department of Energy (Shapiro Report)
Report Date: December 1993
Scope: The Secretary of Energy directed a comprehensive survey and analysis of the new Office of Intelligence and National Security (IS) that was comprised of the previously independent offices of Intelligence, Arms Control and Nonproliferation, Security Affairs and Emergency Management.
Summary: The report identifies roles and responsibility issues within the Department and calls for a defining of intelligence and national security roles, reorienting DOE intelligence priorities, realizing the full intelligence potential of laboratory assets, centralizing R&D and resource management, transferring safeguards and security oversight under IS, examining the security concerns associated with the declassification process, and increasing interaction between emergency management organizations.

Report Title: Report of the Secretary's Safeguards and Security Task Force (Freeze Report)
Report Date: December 1990
Scope: The task force was charged with reviewing the management, planning and operations of the Department's safeguards and security program.
Summary: The key findings of this report are that roles and responsibilities with the Department are unclear and recommends streamlining the security planning

process; improving the personnel security clearance process; increasing the availability of threat information; developing a strategic material control and accountability plan; and completing the required 100 percent inventory of Secret documents.

Report Title: Operation Cerberus, Report of the Committee on International Safeguards and Physical Protection (Cerberus Report)
Report Date: September 1986
Scope: The study was undertaken to review the statutory responsibilities imposed on DOE relating to international safeguards and physical protection.
Summary: The report recommended the centralization of all export control functions, management of international nuclear activities, and technical international safeguards and physical protection functions and responsibilities.

Report Title: Direction for Safeguard and Security (Badolato Report)
Report Date: January 1986
Scope: The memorandum outlines strategic deficiencies with the management of safeguards and security within DOE. The areas of focus are: management, decision making & problem solving, and fitting into the department's corporate management structure
Summary: The premise of the memorandum is that the Department lacks a clear vision for S&S, recommends to establish a doctrinal base and manage from a system-wide perspective (corporately) by developing goals and objectives which support the base; plan framework for action which outlines roles and responsibilities; work in unison and more adaptive to changes; needs to develop its organizational design that is collaborative and focus on goal achievement.

DOE O 414.1, *Quality Assurance*, which establishes requirements for ensuring that DOE work meets requirements and expectations, and that quality improvement is effected through rigorous assessments and effective corrective actions.

DOE O 470.4, *Safeguards and Security Program*, which establishes requirements and responsibilities for managing DOE safeguards and security programs, including managing safeguards and security-related corrective actions.

Presidential Policy Directive/PPD-21, *Critical Infrastructure Security and Resilience*, which establishes a national policy and Federal government roles and responsibilities for strengthening the security and resilience of United States critical infrastructure against physical and cyber threats.

10 CFR Part 830, *Nuclear Safety Management*, which establishes requirements for the conduct of activities that may affect the safety of DOE nuclear facilities.