DOE Science and Security Action Plan Summary

Recommendation	Implemented	In Progress	Under Review
I. CLARIFY LINES OF RESPONSIBILITY AND AUTHORITY			
1. Clarify line management and staff responsibilities	√	√	
2. Clarify federal policy and oversight responsibilities	√	√	
3. Reduce the size of the federal staff		√	
4. Commit to the GOCO management model	√	√	
5. Build an integrated, multi-year budget process	√	√	
6. Assign a single point of responsibility for counterintelligence			√
II. INTEGRATE SCIENCE AND SECURITY			
1. Make implementation of the ISSM policy a top priority	√	√	
2. Ensure laboratory directors have full responsibility for science and security at their sites and are held accountable	√	√	
3. Clarify that security and counterintelligence professionals must provide staff support to line management at all levels of the system	√	√	
4. Revise the directives and other guidance to the laboratories so that they are performance based		√	
5. Ensure that the laboratories are subject to rigorous oversight	√	√	
6. Institute development of a service approach to security management for the labs	√	√	
7. Establish a laboratory security council, chaired by the Deputy Secretary, to provide for the collaborative development of security policies		√	
8. Direct that laboratory directors establish an integrated security group at each site to provide for collaborative implementation of security policies		√	
9. Institute an annual DOE-wide implementation conference to share best practices and address crosscutting problems		√	
10. Establish a program to detail security, counterintelligence, and scientific professionals on a rotational basis to DOE headquarters or the labs		√	
11. Require regular interaction between top DOE management and laboratory directors		√	
12. Establish close coordination at headquarters across security and counterintelligence functions	√	√	
13. Request laboratory directors establish security teams comprising all counterintelligence and security elements at each site		√	
14. Clarify security expectations for line management with respect to their leadership roles and responsibilities on security matters		√	
15. Make security expectations for employees clear, logical, and appropriate to the task	√	√	

DOE Science and Security Action Plan Summary
(Continued)

Recommendation	Implemented	In Progress	Under Review
III. DEVELOP AND PRACTICE RISK-BASED SECURITY			
1. Develop a risk-based systems approach to managing security for the DOE-complex, to be implemented through integrated teams at headquarters and the laboratories	√	√	
2. Provide overarching guidance from headquarters to the sites for the development of integrated safeguards and security plans, including high-level priorities for assets requiring protection	√	√	
3. Direct the laboratories to conduct annual integrated safeguards and security risk assessments and develop plans at the site level, through integrated risk management teams	√	√	
4. In parallel with the fiscal budget, issue an annual DOE enterprise-wide safeguards and security plan, comprised of the individual laboratory plans			√
5. Expand significantly the analytical capabilities of counterintelligence to collect, fuse and analyze data from all sources	√		√
6. Relieve the counterintelligence program of its perceived responsibility for acting as security regulator while encouraging it to strengthen cooperation with the scientific community for information collection and analytical purposes		√	
7. Revise policy for foreign unclassified visits to ensure sound data collection, but also allow laboratory directors to exercise judgment regarding advance screening requirements		√	
8. Ensure that counterintelligence officers have the necessary access to information on foreign nationals at the unclassified, open science laboratories		√	
9. Establish local cooperative agreements between counterintelligence officers and scientists regarding Cooperative Research and Development Agreements		√	
10. Request a National Security Council-led review of PDD-61 to ensure interpretation consistent with the commission’s recommendations			√
11. Issue a comprehensive statement on security policy and principles that authoritatively defines the “zero tolerance” policy by leaving room for reasoned judgment, with the context of maintaining rigorous security		√	
12. Implement a polygraph policy comparable to that of DOD			√
13. Streamline and simplify policies for “sensitive unclassified information” by discontinuing the use of “sensitive unclassified” definitions and labels; directing all laboratories to undertake a systematic review to ensure proper control of classified information under existing guidelines; directing a review of unclassified information not currently subject to statutory administrative controls, for possible placement under a single administrative control category of “Official Use Only” (OUO); ensuring cooperation between counterintelligence officials and the laboratories on unclassified matters of specific concern		√	
14. Seek re-issuance of President Reagan's NSDD-189, to reaffirm that fundamental research is generally exempt from security regulations and that any controls can only be imposed through a formal process established by those regulations			√

DOE Science and Security Action Plan Summary
(Continued)

Recommendation	Implemented	In Progress	Under Review
IV. ADOPT NEW TOOLS AND TECHNIQUES			
1. Invest in new technologies, such as public key infrastructure and biometric systems for access to all cyber systems and for access to all sensitive facilities		√	
2. Invest in databases, information systems and analytical tools to perform extensive fusion, analysis and data mining of authorization, access, biometric, counterintelligence and related data	√	√	
3. Establish processes for applying the above tools and techniques to the visitor request, approval, and monitoring system for visitors to DOE laboratories		√	
4. Establish a small, independent technical team outside the Department of Energy for a limited time (e.g., at an FFRDC), to help develop and refine a risk-based integrated security model		√	
5. Establish a standing security advisory board		√	
V. STRENGTHEN CYBER SECURITY			
1. Assign the Chief Information Officers for DOE and NNSA lead responsibility for cyber security			√
2. Establish a high-level cyber security advisory panel		√	
3. Establish standard operational procedures, appropriate to each laboratory, to measure and provide oversight of cyber network performance		√	
4. Implement classified cyber systems rapidly at DOE headquarters		√	
5. Ensure that developed cyber security solutions are implemented with high priority and emerging technologies are evaluated for possible use		√	