U.S. DEPARTMENT OF ENERGY

CYBER SECURITY ACTION PLAN III

SOUND INVESTMENTS TODAY FOR A SECURE TOMORROW

April 2002

OFFICE OF THE CHIEF INFORMATION OFFICER

U.S. DEPARTMENT OF ENERGY

CYBER SECURITY ACTION PLAN III

SOUND INVESTMENTS TODAY FOR A SECURE TOMORROW

APRIL 2002

OFFICE OF THE CHIEF INFORMATION OFFICER

Table of Contents

EXECUTIVE SUMMARY

The following plan represents the third generation of the Department of Energy (DOE) Cyber Security Action Plan. This plan defines the Office of Cyber Security strategic vision of becoming a national center of excellence for the safeguarding of classified and unclassified information on electronic systems and critical cyber infrastructures. This enormous undertaking encompasses policies, procedures, and implementation efforts throughout a large, diverse, and geographically dispersed organization. The Action Plan lays out a concrete set of projects over a 2-year period.

This plan supports four functional areas and three key goals. These four areas are as follows:

- Planning and Performance Management
- Education, Training, and Awareness
- Engineering and Assessments
- Technical Development.

The three goals are as follows:

- Strengthening the cyber security community
- Strengthening the implementation of DOE's cyber security policies to meet or exceed national standards
- Strengthening the DOE internal cyber security infrastructure

To achieve the goals of the Office of Cyber Security, the following action items will be undertaken over the next 2-year period:

- Continue with the development of the action plan to promote and support DOE's vision.

- Define roles and responsibilities for Headquarters and line organizations.

- Ensure that E-government initiatives are secure and responsive to the public.

- Update the agencywide Cyber Security Threat Statement including new threat information based on recent world events.

- Deploy a DOE-wide performance metrics program to provide an assessment of real-time implementation of cyber security programs and to improve security policies where enhancement is warranted.

- Develop and now maintain and update the Government Information Security Reform Act (GISRA) Plan of Action and Milestones (POA&M) for OMB. This report describes the Chief Information Officer's (CIO) plan to strengthen DOE's cyber security program by ensuring weaknesses identified by internal and external audits are tracked from identification to resolution.

- Develop a cyber security information technology (IT) capital planning process to ensure cyber security dollars are appropriately managed, reviewed, and funded to facilitate the full

integration of security into the IT life cycle.

- Continue with the evolution of DOE cyber security guidance directives.
- Expand the Outreach/Lessons Learned program with the continued publication of the CIO's Office of Cyber Security Cyber Security Daily New Brief and publication of the "best practices" papers.
- Develop and expand a comprehensive DOE-wide cyber training program, including forensics awareness training, a recognition program, and a catalog of courses.
- Continue to support the Computer Incident Advisory Capability (CIAC) in its mission to assist any DOE element that experiences a computer security incident by providing analysis, response, and restoration of operation.
- Expand public key infrastructure (PKI) capabilities throughout DOE to support trusted relationships among all users.
- Fund Secure Telephone Unit-Third Generation (STU-III) replacement at 25 percent of assets annually over the next 4 years.
- Continue to fund DOE-wide infrastructure/architecture upgrades.
- Fund innovative technologies to ensure practical and enhanced cyber security protection capabilities.
- Transition a Counterintelligence project (Intrusion Monitoring Analysis and Correction [IMAC]) that improves the ability to forecast upcoming attacks to the Office of Cyber Security.
- Continue with Step 2 of the Project Matrix Initiative.

1. STRATEGIC VISION OF THE OFFICE OF CYBER SECURITY

The strategic vision of the Office of Cyber Security is to become a national center of excellence for the safeguarding of classified and unclassified information on electronic systems and critical cyber infrastructures. This enormous undertaking encompasses policies, procedures, and implementation efforts throughout a large, diverse, and geographically dispersed organization. Key to the Department of Energy's (DOE) success is a uniform implementation of innovative policies and agile solutions across the entire enterprise, coupled with an effective cyber security education program available to all DOE staff and contractors.

1.1 GOALS OF THE OFFICE OF CYBER SECURITY

The Office of Cyber Security has determined that to become a national center of excellence it must be committed to strengthening the DOE cyber security community, strengthening DOE cyber security policy implementation to meet or exceed national standards, and strengthening DOE's internal cyber security infrastructure. DOE will also continue to develop innovative approaches for confronting newly identified threats to the community's information systems. These challenging tasks will require dedication and perseverance, but DOE's Office of Cyber Security is committed to its vision of excellence.

1.2 ACTION STEPS

This Action Plan describes ongoing and future activities under the DOE Cyber Security Program. Historically, the program's activities or action steps have been organized into four functional areas. These four functional areas serve as the Office of Cyber Security's core competencies and have proven to be a highly effective means by which budget planning and program execution activities occur. When cross-matrixed with its Strategic Goals, the relationship provides a series of traceable links between the Office's capabilities and budget, the initiatives resulting from the matching of those resources, and the strategic goals they support. This Action Plan lays out an integrated set of activities over a 2-year period that provides the foundation necessary for attaining the vision of the Office of Cyber Security through achieving the established goals. As illustrated in Figure 1.1, the action steps are organized into the following four functional areas:

- *Planning and Performance Management.* DOE will continue to provide a sound and comprehensive framework for effective implementation of the Cyber Security Program.

- *Education, Training, and Awareness.* DOE will continue to develop a coordinated training program intended to improve job performance by providing managers and staff with not only a practical understanding of cyber security threats and vulnerabilities but also the skills and capabilities to address them.

- *Engineering and Assessments.* DOE will continue to provide departmental cyber security engineering and assessment resources to support day-to-day computer operations throughout DOE and throughout the life cycle of computer systems and the information

they process.

- *Technical Development.* The Office of Cyber Security's research and technical development capability is designed to research new, innovative cyber security protection capabilities with the goal of improving the Department's information and cyber security systems. DOE will identify, evaluate, and if needed, develop cyber security tools to protect against current and future cyber-related threats and vulnerabilities. DOE will perform need-based analysis to identify new threats and desired protection capabilities. Commercial off-the-shelf (COTS) security software will also be evaluated in a DOE environment, and research and development (R&D) will be conducted to address long-term cyber security needs. DOE-developed tools will be used to provide capabilities not being met by commercial or other government cyber security products.

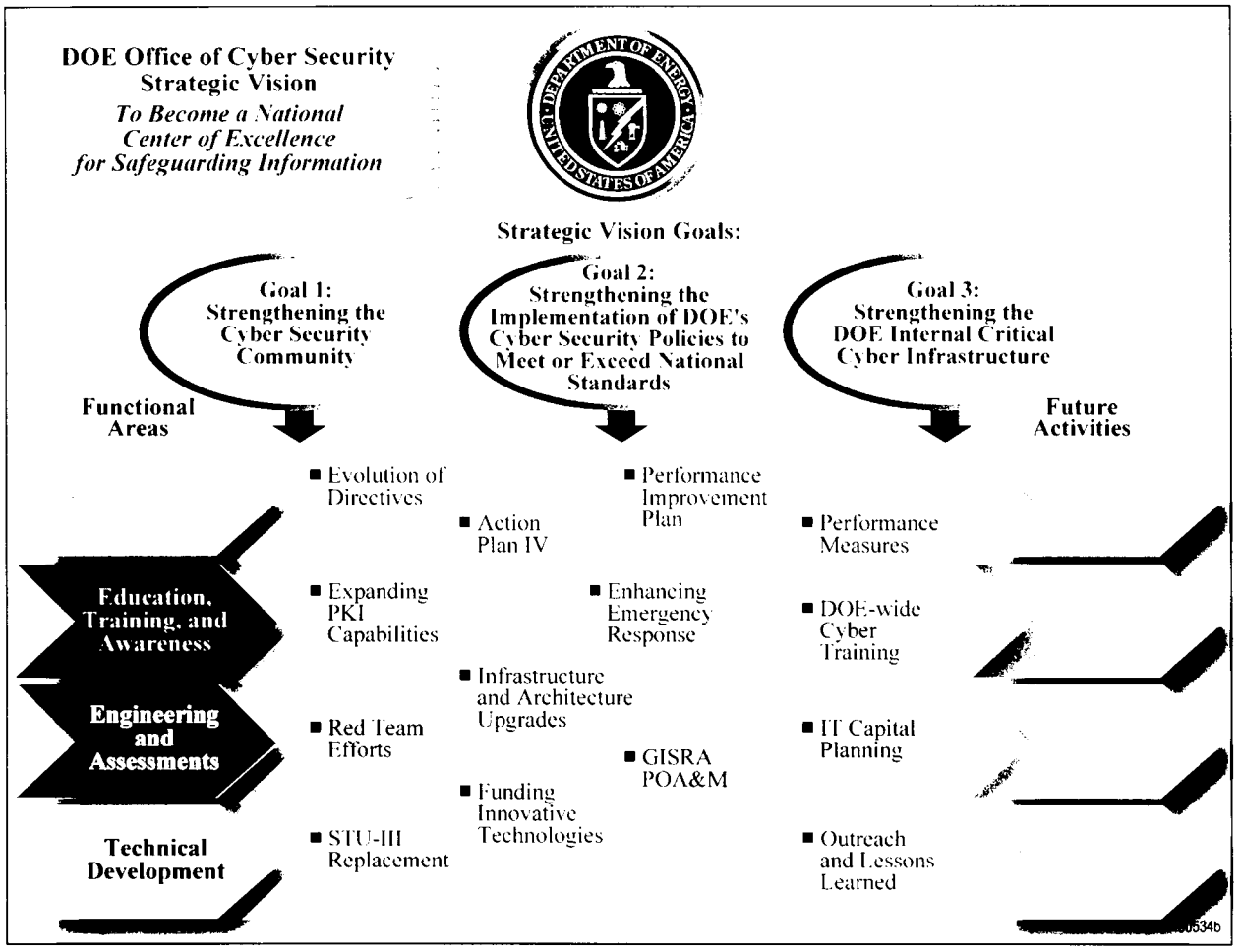


Figure 1-1. DOE Office of Cyber Security Strategic Vision

The Office of Cyber Security has established the following initiatives to support the three main goals of the CIO:

Goal 1—Strengthening the DOE cyber Security Community

1.1 Continue with the development of the action plan to promote and support DOE's vision.

1.2 Define roles and responsibilities for Headquarters and line organizations.

1.3 Ensure that E-Government Initiatives are secure and responsive to the public.

1.4 Update the agencywide Cyber Security Threat Statement to include new threat information based on recent world events.

Goal 2—Strengthening the implementation of DOE cyber security policies to meet or exceed national standards

2.1 Deploy a DOE-wide performance metrics program to provide an assessment of real-time implementation of cyber security programs and to improve security policies where enhancement is warranted.

2.2 Develop and maintain and update the Government Information Security Reform Act (GISRA) Plan of Action and Milestones (POA&M) for the Office of Management and Budget (OMB). This report describes the Chief Information Officer's (CIO) plan to strengthen DOE's cyber security program by ensuring weaknesses identified by internal and external audits are tracked from identification to resolution.

2.3 Develop a cyber security information technology (IT) capital planning process to ensure cyber security dollars are appropriately managed, reviewed, and funded to facilitate the full integration of security into the IT life cycle.

2.4 Continue with the evolution of DOE cyber security guidance directives.

2.5 Expand the Outreach/Lessons Learned program with the continued publication of the CIO's Office of Cyber Security Cyber Security Daily New Brief and publication of the "best practices" papers.

2.6 Develop and expand a comprehensive DOE-wide cyber training program, including forensics awareness training, a recognition program, and a catalog of courses.

Goal 3—Strengthening the DOE internal critical cyber infrastructure

3.1 Continue to support the Computer Incident Advisory Capability (CIAC) in its mission to assist any DOE element that experiences a computer security incident by providing analysis, response, and restoration of operation.

3.2 Expand public key infrastructure (PKI) capabilities throughout DOE to support trusted relationships among all users.

3.3 Fund a Secure Telephone Unit-Third Generation (STU-III) replacement at 25 percent of assets annually over the next 4 years.

3.4 Continue to fund DOE-wide infrastructure and architecture upgrades.

3.5 Fund innovative technologies to ensure practical and enhanced cyber security protection capabilities.

3.6 Transition a Counterintelligence project (Intrusion Monitoring Analysis and Correction [IMAC]) that improves the ability to forecasts upcoming attacks to the Office of Cyber Security.

3.7 Continue with Step 2 of the Project Matrix Initiative.

Table 1-1 provides a brief crosswalk of the activities that support the four functional areas and the strategic goals of the Office of Cyber Security.

Table 1.1. Activity Crosswalk

Functional Area	Goal #1	Goal #2	Goal #3
Planning and Performance Management	1.2 1.3	2.1 2.3 2.4 2.5	3.5
Education, Training and Awareness	1.2 1.3	2.6 2.4	3.1 3.2
Engineering and Assessments	1.1 1.2 1.3 1.4	2.4 2.6 2.4	3.1 3.4 3.6 3.7
Technology Development	1.3	2.2 2.6	3.1 3.2 3.3 3.4 3.5 3.6

2. FUTURE ACTIVITIES

The CIO's Office of Cyber Security has developed a set of projects that will assist DOE in becoming the center of excellence for safeguarding classified and unclassified information on electronic systems and critical cyber infrastructure. This is an enormous undertaking for a large, diverse, and geographically dispersed organization. The CIO is committed to the strategic vision of the Office of Cyber Security, and these future projects will enable DOE to become a center of excellence.

2.1 STRENGTHENING THE CYBER SECURITY COMMUNITY

2.1.1 Continuing With the Development of the Action Plan to Promote and Support DOE's Vision

The Office of Cyber Security will continue to develop an annual Action Plan that can be used as a multipurpose tool for communicating future DOE Cyber Security Program activities to employees, other agencies, and oversight authorities. The Action Plan will describe ongoing and future activities under the DOE Cyber Security Program. The plan will lay out an integrated set of activities to be accomplished over a 2-year period. These activities will provide the foundation necessary for attaining the vision of the Office of Cyber Security.

2.1.1.1 Risk Management. A sound risk management methodology is fundamental to a first-class information security program. To successfully protect DOE's ability to carry out its diverse set of missions, the CIO will develop a sound, flexible, and easily implemented methodology for organizations across the complex to assess risk. The risk methodology will include risk assessment, mitigation, and acceptance. The risk assessment process will include the identification and evaluation of risks, the impact the risk would have on the Department, and control measures that could be incorporated to reduce risk. The risk mitigation process will build on the risk reduction measures identified during the risk assessment process. It will include the prioritization, implementation, and maintenance of the risk reducing measures identified. Finally, processes must be in place to ensure that any remaining risk, which cannot be mitigated, is documented and accepted by an authorized official.

2.1.1.2 Configuration Management. In an attempt to identify and characterize all of DOE's information system components and their relationships in a continually evolving series of enclaves and clusters, the Department will prepare the DOE's Configuration Management Guide. The guide will provide DOE developers, project managers, management teams, and everyday users with the procedures, methods, and tools needed to identify components, establish baselines, control changes to those baselines, record and track the status of changes, and audit the components. The guide will establish the overall strategy and provide procedural guidance to be used by all organizations within DOE. It will also provide guidance in day-to-day configuration management for DOE federal and contractor elements. Finally, the guide will provide a methodology that organizations may use so that changes made in the course of network enclave/cluster development, production, and operation are beneficial, effected without adverse consequences, and managed throughout the entire life cycle.

2.1.1.3 Independent Validation and Verification. The Department plans to develop a comprehensive Independent Validation and Verification (IV&V) Guide that will provide a framework in which computer systems can be independently tested for vulnerabilities to cyber attack. The guide will develop a process for testing and analyzing software and/or systems to detect flaws in design and coding errors that may have eluded quality assurance reviews that took place during the design stage. This guide will serve as a valuable management tool to further reduce the risk of system compromise and failure resulting from security-related vulnerabilities. The guide will offer a formal and structured process to identify the vulnerabilities and serve as a guideline for tests or reviews that are recommended for both COTS products and internal software development efforts. The guide will also be used as a means to establish a baseline IV&V assessment of the organization's existing IT enclaves. The IV&V process will result in the conservation of financial resources, increased accountability, and the CIO meeting or exceeding the national standards in the cyber security arena.

2.1.1.4 Certification and Accreditation Program. The Department plans to expand its Certification and Accreditation (C&A) Program. The program will establish a departmentwide process to certify that an information system or site complies with documented security requirements and will continue to maintain the accredited security posture throughout the system life cycle. The program will include an overview of the process, roles, and responsibilities, and the documentation process involved in the certification and accreditation process. The program will be built on a sound risk management process, which will aid in determining the protection requirements for the information stored or processed on the DOE information system. A management process will allow for an assessment of the consequences of loss of confidentiality, integrity, and availability against the costs of protecting the information.

2.1.2 Defining Roles and Responsibilities for Headquarters and Line Organizations

The Office of Cyber Security will work with Headquarters and line organizations to define their roles and responsibilities to ensure enterprisewide buy-in of DOE's security program. All employees must support a security program for it to be successful. The employees will look to Headquarters and line management for leadership, and they must buy in to the rationale for security and view it as an integral part of their jobs. Clearly defined roles and responsibilities will assist in obtaining this employee buy in. Which will result in a robust security program that is

supported enterprisewide.

2.1.3 Ensuring That E-Government Initiatives Are Secure and Responsive to the Public

The President has made "Expanding Electronic Government" one of his five priorities in his quest to improvement the results of federal IT spending. This E-Government initiative focuses its efforts on making the Federal Government both citizen and results oriented. The goal is to provide information and/or services to the citizens in minutes, rather than the current standard of 2 weeks. The Office of Cyber Security is committed to advancing the President's E-Government initiative while ensuring the security of the information systems employed to move the initiative forward.

2.1.4 Cyber Security Threat Statement

The CIO will issue an updated agencywide Cyber Security Threat Statement, which will include new threat information that has been made available based on recent world events. The Cyber Security Threat Statement provides general threat information concerning DOE's information systems. This statement will provide a baseline of all known risks, which will assist sites in the development of site-specific threat statements.

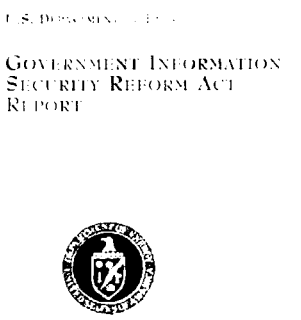
2.2 STRENGTHENING THE IMPLEMENTATION OF DOE'S CYBER SECURITY POLICIES TO MEET OR EXCEED NATIONAL STANDARDS

2.2.1 Performance Measurement

The Office of Cyber Security will launch the Cyber Security Performance Measurement Program, beginning with an initial data call from the Office of Cyber Security. The program will provide the Office of Cyber Security a means to assess the implementation of the cyber security program. The data call will be made twice annually and organizations need only report changes to the initial data call. The analysis of the data will assist the Office of Cyber Security in identifying security policy compliance, as well as policies in need of improvement.

The Cyber Security Performance Measurement Program demands site accountability while giving line management the latitude and flexibility to proactively manage cyber security activities. This approach also meets immediate reporting requirements, and in the long term provides the Department with more control over cyber security implementation.

2.2.2 Continued Improvement of the GISRA Plan of Action and Milestones for OMB



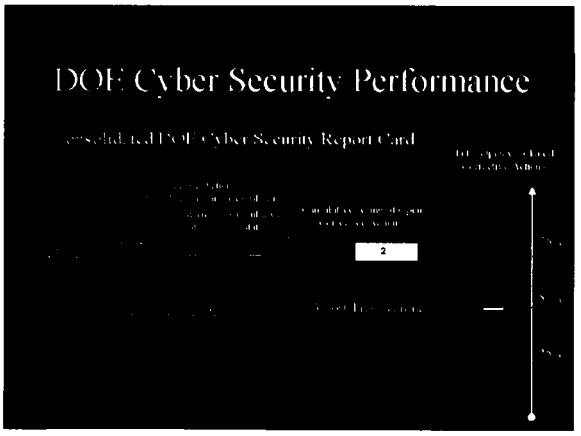
GISRA mandates that the Department provide a POA&M for each major program or system to OMB. The POA&M responds to specific security weaknesses identified within DOE's 2001 GISRA report submission on the status of the Department's overall cyber security. OMB has provided specific guidance on the structure and information requirements for the POA&M report. DOE's POA&M report was written following OMB's guidance, and it responds to specific security weaknesses identified within DOE's 2001 GISRA report on the status of the Department's overall cyber security. The POA&M reflects the Department's commitment to resolving its cyber security weaknesses and shortfalls and that DOE is working diligently to correct those weaknesses. The POA&M will be continuously improved throughout the year and submitted quarterly to OMB.

2.2.2.1 Cyber Security Performance Improvement Plan. DOE's CIO is in the process of developing the Cyber Security Performance Improvement Plan as a response to a recent assessment of federal government computer security released by the Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations. This assessment awarded the Federal Government a grade of "F", including DOE. The grade was based on information that the Department submitted to OMB in response to the GISRA report submitted on September 15, 2001. DOE has received the analysis and scoring criteria, and is in the process of developing the Cyber Security Performance Improvement Plan. The plan will identify those specific actions that will strengthen the Department's cyber security posture and improve DOE's cyber security score with Congress. The plan will also assist in restoring

regulatory and stakeholder confidence in the Department's cyber security program, and integrating corrective actions and apprising management of the status of corrective action completion. This Cyber Security Performance Improvement Plan will be a living document that will assist the CIO in establishing a robust cyber security program that will protect the information embedded in the Department's electronic systems. In addition, the tracking of these actions by the CIO's Office of Cyber Security will provide DOE management with a near-real time snapshot of progress and improvements.

The Office of Cyber Security is now developing an automated Performance Improvement Plan database to simplify the management of the plan. The database will be centrally located at the DOE Knowledge Center and will allow for the Program Support Offices (PSO) to update their respective information via a user-friendly interface. The weakness resolution status will be updated at least once each quarter. Resolution status for any new weaknesses identified through the GISRA reporting process will also be tracked.

2.2.2.2 Department Cyber Scorecard. In conjunction with the Cyber Security Performance Improvement Plan the CIO is in the process of developing the DOE Cyber Scorecard, a tool that tracks DOE's improvements in cyber security performance in near-real time. This tool will illustrate the most recent achievements in the implementation of the corrective actions identified in the Cyber Security Performance Improvement Plan. The scorecard will also track the cumulative progress of the implementation of these corrective actions. The scorecard will provide this data for all PSOs and their respective field offices and will be updated on a monthly basis. This Cyber Scorecard will be used for interoffice and interagency briefings and will be a resource for the annual GISRA Plan of Action and Milestones for OMB.



2.2.3 Developing a Cyber Security IT Capital Planning Process

The Office of Cyber Security has developed and is implementing an IT capital planning and investment control process for its cyber security investments. This process keeps the Office of Cyber Security in compliance with the requirements set forth in the Clinger Cohen Act of 1996, OMB Circular A-130, and GISRA. The goal of the process is to ensure that taxpayers' dollar are managed effectively and that cyber security IT investments are results-oriented and provide adequate security protection. As a first step in this process, the Office of Cyber Security published the IT Capital Planning Analysis and the IT Capital Planning Action Plan.

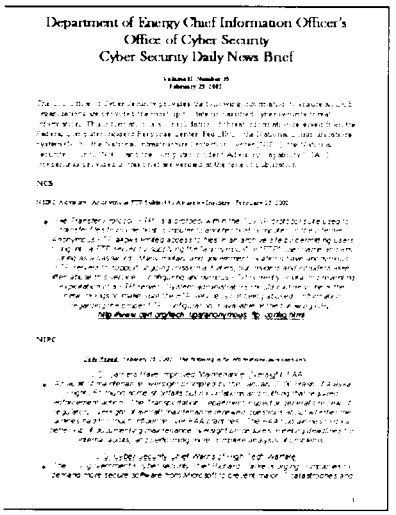
2.2.4 *Continuing With the Evolution of DOE Cyber Security Directives*

In pursuit of the Office of Cyber Security's goal of meeting or exceeding National Standards, the Office of Cyber Security will continue with the evolution of numerous directives, policies and procedures over the next fiscal year. This initiative will involve the revision of classified and unclassified cyber security directives, to include manuals and guides. These revised directives will focus on organizational policy implementation and on legislative or regulatory requirements. Additionally, the Office of Cyber Security will develop a cyber security manual that includes an enhanced Departmentwide warning and reporting capability for the purpose of ensuring the continuity of DOE operations and protecting critical national assets.

During FY 2002, the Office of Cyber Security will continue with the evolution of the following supplemental documents:

- DOE Guide 205.X, Guideline for Cyber Security Penetration Testing
- DOE Guide 205.X, Risk Management
- DOE Guide 205.X, Configuration Management
- DOE Manual 205.X, Certification and Accreditation Manual
- DOE Manual 205.X, Independent Validation and Verification Manual
- Unclassified Cyber Security Threat Statement.

2.2.5 *Outreach/Lessons Learned*


Department of Energy Chief Information Officer's
Office of Cyber Security
Cyber Security Daily News Brief

The Office of Cyber Security is initiating an effort to communicate issues of importance to both the program offices and the field. The office has reviewed recent cyber security internal and external evaluations from a variety of sources, including the Inspector General, Office of Independent Oversight and Performance Assurance, and the U.S. General Accounting Office. This review identified a numerous common areas of concern, and the Office of Cyber Security is planning to publish a series of papers concentrating on the primary concerns. These papers will summarize "best practices" or "general guidance products" for the benefit of the Department's IT community.

The Office of Cyber Security will continue with the publication of the Cyber Security Daily New Brief. This publication provides up-to-date, unclassified, cyber security threat information to all DOE organizations on a daily basis. The information is a compilation of threat information received from the Federal Computer Incident Response Center (FedCIRC), National Communications System (NCS), National Infrastructure Protection Center (NIPC), National Security Council (NSC), and CIAC.

2.2.6 *Developing and Expanding a Comprehensive DOE-wide Cyber Training Program*

The Office of Cyber Security is responsible for training all DOE personnel in cyber security issues. DOE managers and staff are charged with executing precautions to safeguard the information with which they work. They are also expected to recognize cyber abnormalities and execute corrective measures. Consequently, an effective training, education, and awareness program is central to the success of the overall DOE cyber security effort to provide DOE personnel with the knowledge, skills, and abilities to perform as expected. The office will continue the comprehensive training program for all users with access to DOE systems, while simultaneously identifying new training courses that assist in fulfilling job competency requirements. The Office of Cyber Security is developing a DOE Cyber Security training catalog and working with contractors to restructure some courses while developing a DOE-wide cyber security forensics awareness course and a manager's cyber security course.

2.3 STRENGTHENING THE DOE INTERNAL CRITICAL CYBER INFRASTRUCTURE

2.3.1 Participating and Enhancing Emergency Response and Reporting Capabilities for Cyber Assets

The Department will continue supporting CIAC in its mission to assist any DOE element that experiences a computer security incident by providing analysis, response, and restoration of operation. Additionally, CIAC serves as DOE's watch and warning center, notifying the DOE Complex of vulnerabilities being exploited, recommending countermeasures, providing an overview of the current attack profile, and assisting other DOE elements. An analysis conducted of the incident data reported by the Department shows that over the last year intrusion and Web defacements have decreased from 103 incidents in fiscal year (FY) 2000 to 64 in FY 2001. Virus and malicious code incidents have also decreased from 60 to 39 annually. During the same period, the number of scans and probes has increased seven times from 6,407 in FY 2000 to 45,444 in FY 2001. Attempted intrusions were also up from 1,021 to 2,249 during these periods. This shows that although the number of challenges is up over the last FY, DOE cyber security controls have been significantly more effective than in the past. Comparing similar statistics from FY 1999 with the FY 2001 data, intrusions and Web defacements have dropped by more than half, whereas the number of scans and probes has escalated by a factor of 20.

The Office of Cyber Security will continue to provide funding to be used to update or expand the following CIAC services:

- *Incident Response*. Provide the DOE Complex with incident-handling assistance and remediation, including direct technical support to handle computer security incidents and backup support to site response teams handling large and complex incidents.

- *Watch and Warning*. Monitor and report on outside threats to DOE's infrastructure, including new vulnerabilities, new hacker tools, anticipated hacker activities, and potential cyber attacks.

- *Site Security Assessment*. Provide DOE sites with "white hat reviews" and other vulnerability assessments.

- *Cyber Security Tools*. Provide tools and utilities to support security efforts at DOE sites, such as an automated scan detector that automatically reports scanning incidents to CIAC.

- *Training*. Support the Department's cyber security training program by providing information sources and training, education and awareness materials to DOE Headquarters and other DOE sites.

- *Counterintelligence*. Assist and support the Office of Counterintelligence's Cyber (CI-Cyber) pilot program – IMAC Operational Analysis Center (OAC).

- *Inspector General*. Assist and support the DOE Office of the Inspector General as needed.

2.3.2 Expanding PKI Capabilities Throughout DOE to Support Trusted Relationships Among All Users

DOE will enable public key technology capability and an underlying security infrastructure, enhanced by PKI, which will support trusted relationships among users, computers, and applications within the network. The DOE PKI is a foundation for a variety of hardware and software solutions to verify the integrity and originator of data and to provide confidentiality. The PKI architecture consists of Certificate Authorities (CA), Registration Authorities (RA), publicly accessible key repositories, PKI-enabled applications, PKI-enabled services, X.509 digital certificates, trust list relationships between CAs, and the policies that govern operation and use. This architecture exists throughout federal and state government organizations and the commercial business community. This capability will permit secure business processes among all these organizations. In addition, a Federal Bridge capability will provide a means for interoperability across and among business partners. In combination, these PKI components present an opportunity for higher degrees of trust and eliminate some significant legal and technical management issues. The following specific PKI work products have been completed or are nearing completion:

- *Strategy.* In the second quarter of FY 2001, the DOE PKI strategy was finalized and disseminated. The strategy provides an approach for reliable secure sessions, secure applications, and secure device management capabilities. In addition, digital signatures will be incorporated into enterprise systems.

- *Architecture Integration.* DOE has developed and is integrating a PKI architecture that meets all Department requirements and provides scalability and interoperability. The architecture accommodates existing telecommunications channels (i.e., DOEnet) and supports X.500 Directory Services Protocol (DSP) and Lightweight Directory Access Protocol (LDAP). Revisions are being made to the Directory Information Tree (DIT) at participating sites.

- *Implementation Plan.* IM-32 submitted an implementation plan that was reviewed and accepted by the PKI Technical Working Group. The implementation plan has been used as the template for infrastructure integration of X.500 directory services, CAs, RAs, and extended PKI services.

- *Certificate Policy.* A draft Certificate Policy was completed in July 2001. The policy provides for three levels of assurance, including basic-level, medium-level, and high-level assurance certificates. The policy is in the acceptance stage and has been submitted to the National Institutes of Standards and Technology (NIST) for review.

- *Deployment.* As a first phase in deployment, DOE has provided PKI training, services, and support to developers, engineers, and administrators, respective to their function within the PKI infrastructure, to facilitate familiarization, identify potential issues, and facilitate PKI integration into their environments. The PKI training will be extended to personnel with

priority need as defined by the strategy and implementation plans during the deployment's second phase. The third phase will provide for dissemination to all end users.

- *Program Extension.* DOE will continue to deploy RA services, issue certificates, and PKI enable applications throughout Headquarters and to sites that have established a need for such services. DOE will also ensure the deployment of Biometrics and Smart Card services in support of multifactor authentication and high assurance requirements. DOE will extend the PKI architecture to support secure Internet Protocol Security (IPSec) session services (virtual private network [VPN]) and continuity of operations (Thin Client).

2.3.3 STU-III Replacement

National-level direction, distributed in Advisory Memorandum Communications Security (COMSEC) 2-98 on Secure Terminal Equipment (December 1998), states that the current STU-III equipment will be phased out and replaced with secure terminal equipment (STE). To maintain DOE capability to conduct classified conversations using telephones, it is necessary to transition from the STU-III to the STE. In FY 2001, the CIO published the STE Transition Plan that defines DOE's incremental 4-year replacement program of its current STU-III equipment, beginning in FY 2002 and ending in FY 2005, to be conducted at a 25-percent-per-year replacement rate. During this period, support for the STU-III will be phased out and aligned to the transition of STE units.

2.3.4 Infrastructure and Architecture Upgrades

The Department's Cyber Security Architecture (CSA) provides a cyber security framework for the operation of existing systems and development of future systems. The CSA also lays the groundwork for migrating DOE's current networks and information systems to a more secure environment. The CSA guidance, finalized in March 2001, was issued for immediate application by the entire Department for use in reassessing its cyber security posture and formulating an upgrade program. To guide organizations in formulating Cyber Security Program Plan (CSPP) updates and to reflect the changing action-reaction dynamic of security technology, the CSA guidance will be updated biannually. The update will be based on changes in threat, field feedback, audit reports, technology advances, and government and industry best practices.

The following actions will be taken to help implement the CSA:

- *Update DOE Cyber Security Baseline.* Aggregated baseline information derived from organizational CSPPs will be used to monitor and assess organizational cyber security postures. The CSPP baseline database will be updated as new and revised CSPPs are received.

- *Gap Analysis and Program Update.* To implement CSA guidance, the CIO will recommend that the DOE Complex perform a gap analysis to identify where baseline cyber security diverges from CSA guidance and modify CSPPs to reflect the necessary changes.

- *Implementation Monitoring.* The Office of the CIO will review audit and inspection reports for CSA-related findings and trends and will evaluate quarterly progress reports submitted by organizations receiving supplemental funding. To a more limited extent, site assistance visits will be used to obtain first-hand information about how activities are progressing in applying CSA guidance. In addition, monitoring will occur via the annual budget process and through a review of evaluations made by the Office of Independent Oversight and Performance Assessment.

2.3.5 Technology Development

Information technology, an essential supporting element of DOE's mission, is used for all facets of the Department's operations. Cyber security technical development is designed to research new, innovative cyber security protection capabilities and technology with the goal of improving the Department's information and cyber security systems. DOE will identify, evaluate, and if needed, develop cyber security tools to protect against current and future cyber-related threats and vulnerabilities. DOE performs need-based analysis to identify new threats and desired protection capabilities. COTS security software is also evaluated in a DOE environment, and assessments are conducted to address long-term cyber security needs. DOE-developed tools are used to provide capabilities not currently met by commercial or other government cyber security products.

The technical development program is well coordinated and highly leveraged within DOE. The CIO's investment in the technical development program in FY 2001 allowed for the evaluation of five leading sanitization products against National Industrial Security Program Operating Manual (NISPOM) criteria, resulting in the issuance of interim guidance to the field. The CIO also completed an independent assessment of the use of A/B computer switches at Headquarters. Additionally, an assessment of Safepatch, an automated security patching program for information systems, was completed that resulted in DOE's endorsement of the product.

2.3.5.1 Connection Log Analysis (Logger). The Connection Log Analysis, also known as Logger, is an automated collection and analysis tool used for monitoring network traffic. Logger provides an automated collection of multiple network connection logs, database storage, and automatic analysis of the logs using an advanced correlation analyses for evidence of intrusive or threatening activities. It is believed that the ability to correlate connection logs from multiple DOE sites will provide more information about potential intruder activities than the analysis of individual connection logs. The use of Logger will result in fewer undetected intrusions and early warning of impending intrusions, which will ultimately result in a better security posture for DOE networks.

2.3.5.2 Network Intrusion Detector. The Network Intrusion Detector (NID) monitors network traffic on local segments for indications of suspicious activities or connections. NID's unmatched strength is its ability to quickly and accurately match exploitation signatures against the datagram portion of a packet. A primary goal of this project is to expand the NID capabilities to detect attacks that are based on packet header content. NID currently presents several distinct advantages to DOE sites: runs in real-time, has little or no operational effect on the network or associated systems being monitored, provides retrospective analysis, and successfully detects multiple attack types.

2.3.5.3 Multiplatform Trusted Copy Enhancements. Multiplatform Trusted Copy (MPTC) Enhancements is a field-user focused project that adds needed functionality to the base MPTC product. MPTC is a software tool that permits close examination of computer files before executing a special transfer of those files, typically from classified environments to unclassified. Recent changes in DOE Classified Computer Security requirements mandate, among other procedures, that a two-person check be performed on all file transfers from the classified to unclassified domains. MPTC is well suited for this requirement but will require enhancements to provide additional automated assurances of valid two-person checks.

Hidden information exists in modern file formats (some of which could be sensitive information), requiring each file format to be explicitly "understood" by MPTC in order for a rigorous analysis of the file to be performed. The initial file formats that MPTC understands are Microsoft Word97, Excel97, PowerPoint97, and numerous text-based file formats (such as computer aided design [CAD] files). The MPTC Enhancement effort focuses on expanding the numbers of file types understood by MPTC to include those in MS Office 2000. User requirements drive the priorities assigned to these file formats, and users are strongly encouraged to express their preferences for certain file format templates.

A number of additional security risks exist that may adversely affect secure file transfers. Data and functionality may be embedded in files using techniques such as steganography and intelligent software agents. These embedding techniques are difficult, if not impossible, to detect without specialized tools.

Proposed for FY 02 under this project is to provide MPTC version 2.0, including—

- Software requirements (SRD) and software design (SDD) documents that describe the enhancement features
- Research key signature(s) associated with intelligent agent code and provide a multiplatform, first-order intelligent agent recognition capability integrated into MPTC (a significant research component is associated with this task)
- MS Office 2000 file format library definitions into MPTC
- Win2000 compatibility
- Security features, such as digital signature or encryption protection, to MPTC session,

review and transfer log files to prevent potential insider tampering

- Ongoing maintenance and field-user support of the MPTC product

- Support for ISPM and other DAA approval activities.

2.3.5.4 Tumbleweed Secure Messaging. E-mail now conveys vital business information, ranging from research documents to invoices to contracts and engineering designs. The confidentiality and integrity of these communications must be preserved. Receiving e-mail messages, opening attachments, navigating Web sites—these basic skills are now second nature to millions of federal employees. As a result, federal employees now expect more and more services to be delivered with Internet convenience and at Internet speed. Because most communication between agencies and their citizen groups concerns sensitive, private, and other confidential information, DOE employees communicating online must ensure that they have the means to securely deliver and receive information from all sources. The task will establish, implement, and maintain a comprehensive and effective cyber security and secure messaging infrastructure to protect the Department's sensitive unclassified and classified information and information technology assets. Tumbleweed's secure messaging solutions will accomplish the following:

- Scan all inbound and outbound messages and attachments for viruses or malicious mobile code.
- Scan outgoing messages to ensure they comply with DOE regulations and government policies.
- Protect data from all DOE sites, while simplifying the authentication of senders and receivers.
- Support Secure/Multipurpose Internet Mail Extensions (S/MIME), PKI, and other authentication schemes such as passwords.
- Archive all messages or any subset of messages specified by administrators.
- Work with any combination of standard e-mail programs and Web browsers, with no need for client side software, lowering support costs.
- Provide a Secure Inbox in which an employee can receive all correspondence. Documents, personal messages, responses to customer service inquiries—all communication from the agency—arrives here.
- Automatically route e-mail messages authored in traditional e-mail programs, such as Lotus Notes into the Secure Inbox.
- Extract data from legacy systems and print streams for formatting and delivery as statements.

The following tasks are proposed for FY 02 under this project:

- *Strategy.* A Strategy document will be drafted for an effective antivirus program that will include protection from malicious code introduced through e-mail.

- *Architecture Integration.* DOE will develop an architecture that meets all Department requirements and provides scalability and interoperability for the protection of transmitted data.

- *Implementation Plan.* DOE will submit an implementation plan for review and acceptance by the cyber security community. The implementation plan will be used as the template for infrastructure integration of antiviral solutions, including e-mail.

- *Deployment.* As a first phase in deployment, DOE will identify sites to participate in the virus protection program. Training will be extended to personnel as defined by the strategy and implementation plans. A proof of concepts will be integrated, and a pilot program will be established thereafter. Upon successful conclusion of the pilot program, services will be deployed to all participating sites.

2.3.5.5 Telecommunications Security Engineering. Telecommunication Security Engineering is responsible for assessing Departmentwide security requirements, ensuring compliance with national level policy (COMSEC and TEMPEST), defining solutions to meet those requirements, developing proof of concepts, conducting pilots, and developing policy and procedural controls for the adopted security technologies. This program is key for ensuring that DOE meets legislative requirements, governmental guidance, and compliance with best business practices for the Department.

The program encompasses COMSEC, emissions security (TEMPEST), and other protection measures for telecommunications. Under the provisions of the TEMPEST program and existing National Security Agency (NSA) requirements, the Department must upgrade its existing, outdated TEMPEST assessment equipment. This effort is necessary in order to continue to provide effective emanations detection and analysis services for DOE. TEMPEST inspections will also be performed to ensure departmentwide compliance to DOE policy and procedures governing the emissions security program. Annual awareness training will be made available to the community. The CIO's Cyber Security Office conducts DOE-wide COMSEC inspections, administration, assistance, and maintenance to ensure that DOE COMSEC activities comply with NSA requirements.

DOE is also responsible for multifactor authentication and common access services. These services are required for support of governmental guidelines established by the Federal Bridge and General Accounting Office (GAO).

DOE will ensure that session encryption will comply with Federal Information Processing Systems (FIPS) requirements and NSA recommendations for security in depth.

DOE will comply with the President's management agenda by ensuring compliance for continuity of operations using technologies such as Thin Client services to protect against manmade or natural disasters.

DOE will comply with NIST requirements for the implementation of the SHA-1 signing algorithm into Web application environments.

DOE will ensure protection that portable code (i.e., virus definitions, system updates) is free of malicious or virus infected code and is digitally signed by a trusted authority.

2.3.6 *Intrusion Monitoring Analysis and Correction*

IMAC is a system designed to provide DOE with an enhanced perspective of security events across the DOE complex in near real-time with sensor development and deployment that will enhance DOE's ability to evaluate and respond to network security issues. This program will result in the deployment of consistent intrusion detection capability at DOE facilities. The system will be placed outside each site's network protection devices, will collect information about in/outbound sessions, and will forward the data to a central location co-located with the Office of Counterintelligence Operational Analysis Center located at Pacific Northwest National Laboratory (PNNL). The data will be analyzed by DOE's Office of Counterintelligence and CIAC.

IMAC's FY 2002 planned activities are as follows:

- Deploy sensor devices at IMAC sites
- Complete training and documentation materials
- Install a new data distributor system at PNNL
- Begin engineering on the data analysis center.

2.3.7 *Project Matrix Step II*

DOE is currently investigating the implementation of Step II for Project Matrix. Ideally, Step II of Project Matrix will take the high level national critical asset defined in Step I and develop a nodal diagram of interdependencies between each critical assets and the public sectors served by these critical assets. Upon completion of this phase of the analysis, the methodology may be applied to other critical assets from Step I to determine an overall strategy to provide enhanced safeguards for these assets. The Office of Cyber Security will participate in the development and implementation of two pilots to test the process.

3. YEAR IN REVIEW

On January 18, 2001, the Secretary of Energy directed that a review be conducted in response to the interim assessment of science and security at DOE laboratories by Dr. John Hamre, the Chair of the Congressional Commission on Science and Security. Subsequently, on January 19, 2001, Under Secretary Gordon issued a memorandum to the National Nuclear Security Administration (NNSA) wherein he directed a review of security policies and directives that had been issued over the past year and a "6-month hiatus from the implementation of new security requirements." The Office of Security and Emergency Operations concurred with this initiative, offered assistance in the conduct of the review, and is participating with NNSA, Defense Programs, and the Office of Science and Counterintelligence in the review. As part of this review, six working groups were established to review the various security policies and directives mentioned above. The working groups focused on the following areas: Foreign Visits and Assignments, Unclassified Nuclear Information, Tri-Lab 9/6 Measures, Enhancement Protective Measures, Unclassified Cyber Security Program, and Sensitive But Unclassified Information. An integrated report from the working groups summarized their findings and recommendations of the reviews.

Evidence of DOE's improved security efforts is found in a recently completed Congressionally mandated Red Team review of the Department's weapons laboratories' sensitive and classified systems and networks. The review showed that DOE had implemented a reasonable level of protection, and the Red Team was unable to penetrate any networks with classified or sensitive but unclassified information. Also, recent U.S. GAO and Office of Independent Oversight and Performance Assessment reviews have highlighted the positive changes that have taken place at many DOE sites. These reviews show that each DOE organization has focused on improving awareness of cyber security threats and implemented improved security controls.

The importance of information security can be seen in the recent restructuring by the newly appointed Secretary of Energy Spencer Abraham making the CIO position a direct report to the Office of the Secretary. This change to the management structure makes the CIO a full participant on the Department's executive management team and further defines the roles and responsibilities of the CIO.

The following is a summary of specific actions taken by DOE since the spring 2000 to improve the level of cyber security:

- Established cyber security policy and technical working groups to assist in formulating policy and guidance and providing technical advice to the CIO
- Provided $12.7 million for Cyber Security Architecture upgrades for various field offices
- Developed and piloted the Cyber Security Performance Measurement Program, which enables the evaluation of cyber security progress at the sites
- Issued a Departmentwide Cyber Security Architecture to provide a cyber security

framework for the operation of existing systems and the development of future systems

- Continued with the development and evaluation of site-specific CSPPs describing the implementation of cyber security protection at the sites
- Deployed Departmentwide training to improve the cyber security skills and knowledge of systems administrators, managers, and contractor personnel
- Continued to expand the PKI initiative, including publishing the PKI Strategy, Implementation Plan, Certificate Policy, and Architecture
- Cross-certified major laboratories for PKI
- Upgraded DOE site cyber security protection through the expanded use of firewalls and intrusion detection software, stronger passwords, improved system configuration controls, and reconfiguration of system and network connectivity to reduce vulnerabilities.

DOE published a comprehensive Departmentwide cyber security management program, Order 205.1, that integrates not only risk management processes, but also physical, technical, and administrative controls for ensuring confidentiality, integrity, and availability of DOE's information assets. Under this program, a framework of objectives, guiding principles, and security activities and functions, which are applicable to classified and unclassified environments, are established to govern consistent implementation of cyber security management throughout the Department.

In summary, the current DOE Cyber Security Program bears little resemblance to the program set in place in the spring 1999. The Department has promulgated updated cyber security policies, improved the effectiveness of its security training for its system administrators, and informed management of upgraded cyber security threats. Each DOE site has a CSPP that identifies its security controls and planned upgrades. Finally, the Department has instituted a review and follow-up process using the Secretary's Independent Oversight function to permit an objective assessment of its status.

4. CONCLUSION

DOE has made a dramatic shift in its approach to cyber security. The plan now reflects the view of the Office of Cyber Security that effective cyber security is a balance of managed policies, procedures, technology training and personnel. This plan is also sensitive to the new E-Government initiatives of providing the citizens with easier access to government services while providing security for our electronic information.

Our strategic vision of being a center of excellence for cyber security is the theme that ties the four functional areas with the specific intermediate goals of strengthening the cyber security community, the cyber security policy implementation, and the internal cyber infrastructure.

We are fortunate to have several internal development efforts that are now ready to be tested in pilot programs with the objective for full rollout later in the year. We continue to support outreach and training programs to "get the message out" that security is the responsibility of everyone in the organization.

In summary, this plan is significantly more complex and far reaching than its predecessors. DOE understands that one office alone cannot dictate or mandate success. Only through a common vision supported by all DOE offices can we truly become a center of excellence.

APPENDIX A -CYBER SECURITY PROGRAM MASTER SCHEDULE