Department of Energy
Washington, DC 20585

July 26, 1999

MEMORANDUM FOR: LEAD PROGRAM SECRETARIAL OFFICES

FROM: JOHN M. GILLIGAN
CHIEF INFORMATION OFFICER

SUBJECT: UNCLASSIFIED COMPUTER SECURITY PROGRAM

DOE N 205.1 UNCLASSIFIED COMPUTER SECURITY PROGRAM has been issued. This notice cancels DOE 1360.2B, UNCLASSIFIED COMPUTER SECURITY PROGRAM, dated 5-18-92. This notice is effective immediately.

The policy is issued as a notice and additional policy and guidance will be required in the area of unclassified computing. This will be worked in a rapid fashion and will be issued upon completion.

Please forward any comments to Pete Salatti, of my staff, 301-903-4477, E-mail pete.salatti@hq.doe.gov.

cc: All Departmental Elements

Department of Energy
Washington, DC 20585

JUN 2 6 1999

MEMORANDUM FOR: JOHN M. GILLIGAN
CHIEF INFORMATION OFFICER

FROM: JOHN WILCYNSKI, DIRECTOR
OFFICE OF FIELD INTEGRATION

SUBJECT: Field Management Council Review Request, 9906-MA011.000

REFERENCE: Memorandum Entitled, "Department of Energy Notice DOE N 205.1, Unclassified Cyber Security Policy"

The Lead Program Secretarial Offices (LPSO) have reviewed your request through the Field Management Council (FMC) process and the Deputy Secretary has approved the issuance of the subject memorandum as revised.

Your office is now authorized to issue the memorandum to the field elements with copies to the LPSOs and Field Integration (FI). All information provided to the field, the LPSOs, and FI should be transmitted electronically.

If you have any questions or comment concerning this action, contact the Office of Field Integration, Skip Castro, at extension 6-4937.

Attachment

cc: DP-1
EM-1
SC-1
EE-1
FE-1
NE-l
RW-1
MD-l
NN-1

Print

U.S. Department of Energy
Washington, D.C.

NOTICE

DOE N 205.1

Approved: 7-26-99

SUBJECT: UNCLASSIFIED CYBER SECURITY PROGRAM

1. OBJECTIVES.

   a. To establish the framework for the Department of Energy (DOE) Unclassified Cyber Security Program.

   b. To set forth requirements and responsibilities for protecting all unclassified DOE information and information systems in order to maintain national security and ensure that DOE business operations proceed effectively.

   c. To ensure that the DOE Unclassified Cyber Security Program achieves the objectives of Federal and State regulations, Executive Orders, national security directives, and other regulations.

   d. To establish best business practices (i.e., requirements) for protecting DOE information and information systems, which include provisions for ensuring that the protection of information systems is commensurate with the risk and magnitude of harm that could result from the loss, misuse, disclosure, or unauthorized modification of information processed, stored, or transmitted using the Department's information systems.

   e. To ensure that the confidentiality, integrity, availability, and accountability of information is preserved by any information system that is used to acquire, store, manipulate, manage, move, control, display, switch, interchange, receive, or transmit that information.

   f. To establish an agile approach to DOE information processing systems security to keep pace with rapidly changing threats, vulnerabilities, missions, and technologies.

   g. To require that Department-wide guidance on the Unclassified Cyber Security Program is updated on a continuing basis.

DISTRIBUTION:	**INITIATED BY:**
All Department Elements	Office of the Chief Information Officer

h. To require that each DOE Headquarters and field element, to include DOE Federal organizations and DOE contractor organizations, tailors the protection mechanisms, implementation, and security planning for its Unclassified Cyber Security Program to suit its environment, missions, and threats, while maintaining consistency and interoperability within applicable mission interoperability clusters.

i. To implement the requirements of Office of Management and Budget, Circular A-130, Appendix III.

2. CANCELLATION. This Notice cancels DOE 1360.2B, UNCLASSIFIED COMPUTER SECURITY PROGRAM, dated 5-18-92.

3. APPLICABILITY.

a. This Notice applies to all DOE Headquarters and field elements, including Federal organizations (hereinafter referred to as DOE elements).

b. This Notice applies to all DOE contractors. Contractor requirements pertaining to the Unclassified Cyber Security Program are listed in the Contractor Requirements Document (CRD), Attachment 1.

c. In this Notice, DOE elements and DOE contractors are collectively referred to as DOE organizations.

4. REQUIREMENTS.

a. Implementation.

(1) This Notice must be implemented by all DOE organizations no later than 180 days after issuance, throughout the Department, by means of contract or financial assistance agreements, specific performance criteria, and a performance measurement system. For DOE organizations not managed by a contractor, implementation must occur upon completion of accepted performance measures determined by agreement with the CIO. Extensions to the 180-day limit will be determined on a case-by-case basis by the CIO.

(2) Additional performance measures may be required for the following specific categories of unclassified information:

- Unclassified Controlled Nuclear Information (UCNI),
- Naval Nuclear Propulsion Information (NNPI),
- Privacy Act Information,

- Export Controlled Information, and
- Information marked "Official Use Only (OUO)."

b. Cyber Resource Protection. Each DOE organization must ensure that all DOE unclassified information resources under its purview are protected in a manner that is consistent with its threats and missions at all times.

c. Risk Management. DOE organizations must use a risk-based approach to identify information resources. A documented risk assessment process must be used to make informed decisions related to the adequacy of protection, cost implications of further enhanced protection, and acceptance of residual risk.

d. Protection of Non-DOE Information. All DOE organizations must protect the information and information technology resources of other Federal Departments and agencies, State and local governments, and entities in the public sector.

e. Resources. In coordination with the respective Lead Program Secretarial Officer (LPSO) and other Headquarters organizations, each DOE organization must plan, budget, allocate, and execute resources sufficient to ensure comprehensive implementation and maintenance of that organization's computer security program.

f. Cyber Security Program Plan. Each DOE organization must document its Cyber Security Program in a Cyber Security Program Plan (CSPP). The CSPP must be approved by the DOE organization's operations, field office, or responsible Headquarters Organization manager following consultation with the DOE Lead Program Secretarial Office (LPSO), Office of the Chief Information Officer (CIO), and the Office of Independent Oversight and Performance Assurance (Independent Oversight). Normally, within 30 days of receiving it, the CIO and Independent Oversight will approve the proposed CSPP or suggest revisions. DOE organizations may revise their CSPPs as required by new operational considerations, risks, vulnerabilities, etc. DOE organizations must submit the revised CSPP to the organization's operations, field office, or responsible HQ organization manager for approval. In urgent situations, they may anticipate approval and implement these revisions while waiting for formal approval.

If an organization is not under the purview of an operations or field office manager, the responsible DOE Headquarters organization must approve the CSPP. The DOE operations, field office, or responsible HQ organization manager is responsible for disposition of the approved CSPP, including submitting a copy of it to the Office of the CIO, which must maintain a current copy of each organization's CSPP. Each DOE organization must provide copies of the draft and approved CSPP to Independent Oversight. At the request of the Office of the CIO, the Independent Oversight will review selected draft plans and provide informal comments on them to the Office of the CIO and to the organization's operations, field office, or HQ responsible organization manager.

g. CSPP Assessment and Review. To ensure that the CSPP is properly implemented, the following three-level review process is used.

(1) Organization Self-Assessment. As called for by the CSPP, but no less frequently than once every 2 years, each DOE organization must evaluate its conformance with the approved CSPP. The evaluation must include a threat and risk assessment and a vulnerability analysis of the information systems identified in the organization's CSPP. The evaluation must also describe the residual risk accepted by the DOE organization manager. If the DOE organization manager is a contractor, the results of the evaluation must also be provided to the operations/field office manager, who is jointly responsible for accepting the residual risk. The DOE organization manager and the operations or field office manager may delegate formal acceptance of the risk, but they retain ultimate responsibility for security of the information systems and the information processed in the systems.

(2) Peer Review. At least once every 3 years, a peer organization must evaluate each DOE organization's CSPP and that organization's conformance with its CSPP. The results must be provided to the DOE organization manager and the Office of the CIO, and in those cases where the DOE organization manager is a contractor, the results must also be provided to the operations or field office manager. Peer reviews may be combined with self-assessments at the discretion of the DOE organization.

(3) Oversight review: Independent Oversight shall maintain a continuous program of independent oversight for cyber security. The independent oversight program will include announced and unannounced cyber security inspections, followup reviews, remote testing for network vulnerabilities (network scanning), and penetration testing. These reviews will assess the effectiveness of the cyber security protection program in meeting the requirements and intent of this directive and the organization's CSPP. Independent Oversight shall notify the cognizant DOE organization manager, LPSO, CIO, Office of Counterintelligence, and where applicable, the operations/field office manager of announced inspections. Independent Oversight will inform the Office of the CIO, Office of Counterintelligence, and the Computer Incident Advisory Capability prior to performing penetration testing on any site's computer systems. Results of each Independent Oversight review shall be provided to the same individuals and may include ratings of program effectiveness and issues requiring development and implementation of corrective action plans.

h. Corrective Action Plans. Each DOE organization must draft and implement corrective action plans to address security shortfalls uncovered as a result of the oversight review process. The corrective action plans must include actions to be taken, responsible organizations and individuals for each action, the schedule (including key milestones), actions to address root causes and generic applicability, a process for tracking actions to closure, and steps to verify effectiveness of actions prior to closure.

i. CIO Groups. To ensure that DOE policy and guidance are appropriate and current, two DOE cyber security groups must be established: the Technical Review Group and the Policy Planning Group. These groups will assist the CIO in developing guidance and recommended approaches for individual DOE organizations and DOE Program Secretarial Offices (PSOs) to use in fulfilling their respective responsibilities for ensuring adequate protection of DOE information resources. Both groups must be selected by the Office of the CIO, following a CIO-determined nomination process, and will be chaired by the Office of the CIO.

(1) The Technical Review Group must, on a continuing basis, assess technology issues, ascertain best security practices, and evaluate the changing nature of threats facing DOE and its organizations. The Technical Review Group will include representatives from DOE, its contractors, and other non-governmental participants who can provide the necessary technical insight and guidance.

(2) The Policy Planning Group must provide policy and best practice recommendations to the CIO. Its members will be drawn from throughout the DOE, including both Federal and contractor personnel.

j. User Authentication. DOE organizations must employ user authentication techniques before allowing users to access systems that support multiple user accounts or that contain hard-to-replace or sensitive data. The organization's CSPP must indicate the systems or enclaves that require authentication and the type of authentication that must be employed.

k. Access Protection. Access to a DOE organization's information resources must be protected commensurate with the risks and threats of its environment. The CSPP must specify the information resources to be protected and the protective mechanisms to be used.

l. Auditing. DOE organizations must be capable of recording, and maintaining in an audit trail, information regarding access to and modifications of all information resources, where this is identified as appropriate by risk and vulnerability analysis, and such capability is technically feasible. The CSPP must state the systems or enclaves that must be audited, what information must be captured in that audit trail, and how long the audit trail must be maintained.

m. Continuity of Service. DOE organizations must employ procedures and mechanisms to curtail or recover from activities that can disrupt or otherwise interfere with system availability, where operationally necessary and technically feasible. The CSPP must identify the organization's systems and enclaves that require such mechanisms and procedures and must detail the procedures and mechanisms employed.

n. Security Monitoring. DOE organizations must report security incidents to the organization incident response team and to the Computer Incident Advisory Capability (CIAC). In addition, each DOE organization must provide 24-hour-a-day, 7-day-a-week coverage. The CSPP must specify the type of events that require monitoring, the enclaves and systems that will be subject to monitoring, how the 24x7 monitoring will be handled, and the composition of the organization incident response team. DOE organizations must also provide security incident information to the National Infrastructure Protection Center (NIPC) and the DOE Office of Counterintelligence as necessary, in accordance with all agreements.

o. Response. DOE and contractor personnel must respond to CIAC cyber security advisories, bulletins, alerts, and suspected incidents in accordance with the policy and procedures stated in the organization's CSPP. The specific response must be commensurate with the perceived level of risk and may include containment, remediation, and increased monitoring. DOE organizations must coordinate joint responsive activities, and the CIO must direct responsive activities throughout DOE, as circumstances warrant.

p. Training. Personnel from all DOE organizations and contractors must be appropriately trained in cyber security vulnerabilities, threats, protection strategies, and respective organizational and personal responsibilities. The CSPP must specify the details of the training program.

q. Malicious Code. Each DOE organization must establish procedures and mechanisms, consistent with the threat environment, to limit (as technically feasible) the introduction of malicious code into its information systems. The CSPP must specify the mechanisms used to detect and prevent the installation of malicious code and the frequency of updating such mechanisms.

r. Mission Interoperability Clusters. To facilitate consistency of security implementation among the DOE organizations, five specific mission interoperability clusters have been defined (see definition in Attachment 2). The CSPP must specify the mission interoperability clusters applicable to its mission and environment.

s. Protection of Classified Information. Classified information must not be entered into unclassified information systems.

t. Major Applications. For major Departmental applications where there is significant risk and where the application resides at multiple sites, it must be determined if a separate Computer Security Program and Computer Security Program Plan must be developed and implemented. The responsible LPSO, in coordination with the CIO, will be responsible for identifying Major Departmental Applications which require a separate Computer Security Program.

u. CSPP Contents. The CSPP for each DOE organization must detail the approach to ensuring effective cyber security. The CSPP must account for the organization's specific environment, missions, and threats. At a minimum, each CSPP must be developed in accordance with all applicable policies, manuals and memorandums and address the following aspects of security.

(1) Define and assign cyber security roles and responsibilities.

(2) Define and describe cyber boundaries and boundary protection techniques, including the scope, specific security policies, connections external to an organization or identified enclave, and protection mechanisms required.

(3) Describe configuration management policies and practices, including a description of the process for making significant changes to the information system architecture and the organization's definition of "significant changes."

(4) Describe the following:

(a) the policy and procedures for responding to incidents at the organization, enclave, or system level as appropriate and in coordination with the Computer Incident Advisory Capability, and reporting to OCI and the NIPC,

(b) the procedures for disseminating and responding to advisories and lessons learned that are forwarded by the CIO or CIAC or generated at the site, and

(c) the composition of the organization incident response team.

(5) Describe the type of changes in technology, threat environment, or other changes to the organization, enclave, or system environment and architecture that would require the CSPP to be updated prior to its normal 2-year cycle.

(6) Describe the cyber security controls (technical and non-technical) employed to ensure confidentiality, integrity, availability, and accountability as required to accommodate the specific threats identified for information entered, processed, stored, displayed, or transmitted. These include, but are not limited to, the following:

(a) Authentication: Describe the type of authentication mechanisms employed, identify the systems and enclaves that require authentication, and, for those systems and enclaves that do not require user authentication, provide a rationale for said decisions.

(b) Access Protection: Describe the access control processes and procedures employed at the DOE organization, which include, but are not limited to–

1 identification of those information systems that require isolation or protection;

2 a summary of strategy for securely accessing enclaves from locations outside of the enclave (including locations both inside and outside of the DOE organization); and

3 a description of circumstances under which penetration testing may be used to validate access protection mechanisms.

(c) Audit: Specify the enclaves, systems, and services (including email) that will be subject to auditing, what information must be collected, and how long audit information must be maintained.

(d) Security Monitoring: Describe the type of events for which monitoring must be employed, which enclaves, clusters, and systems are subject to monitoring, and how 24x7 monitoring must be handled.

(e) Continuity of Service: Identify those enclaves and systems that, due to mission operation necessities, have a low tolerance for disruption or unavailability; describe the procedures and mechanisms that will be employed to limit (as technically feasible) and recover from such disruption or unavailability.

(7) Describe the process for ascertaining the current operational threat, risk, and vulnerability posture; the description must specify:

(a) who (by title/position) within the organization conducts the threat, risk, and vulnerability assessments;

(b) how such threat, risk, and vulnerability assessments are to be conducted; and

(c) how frequently such assessments must be conducted.

(8) Describe the methodology being used for training (e.g., briefings, email), specify how frequently re-training should occur, identify those positions requiring training, and identify (by title/position) those responsible for overseeing training activities at the contractor's organization.

(9) Describe the approach employed to address malicious code (e.g., handled at boundary, handled at desktops, and handled at selected locations), the mechanisms employed, and frequency of updating anti-malicious code software.

(10) Describe the metrics employed to assess compliance with the CSPP and the process for evolving these metrics.

(11) Describe the process for selecting peer members to review the contractor's CSPP and its compliance with the CSPP. The description should include qualifications required of the prospective individuals or entities and who makes the selection.

(12) Identify those mission interoperability clusters that apply to the DOE organization.

(13) Identify the DOE organization manager by title or position.

5. RESPONSIBILITIES.

a. Chief Information Officer (CIO).

(1) Develops Departmental cyber security policies and guidance.

(2) Maintains DOE-wide cognizance of cyber security resources.

(3) Advocates cyber security funding, as appropriate.

(4) Directs DOE-wide activities in response to cyber incidents in coordination with OCI, as circumstances warrant.

(5) Reviews selected CSPPs.

(6) Coordinates with the LPSOs to monitor implementation of DOE cyber security programs.

(7) Coordinates with the LPSOs to facilitate establishment and implementation of needed DOE-wide technical security interoperability standards.

(8) Coordinates with the LPSOs to develop program-specific cyber security policies, guidance, and procedures.

(9) Coordinates with CIAC, the LPSOs, and the Office of Counterintelligence in establishing DOE incident reporting policy and standards.

(10) At the CIO's discretion, participates in Independent Oversight-scheduled inspections and assessments to collect information that may be useful in developing or modifying policies and guidelines.

(11) Defines a nomination and selection process for Technical Review Group and Policy Planning Group membership.

(12) Chairs the Technical Review Group and the Policy Planning Group.

(13) Establishes cyber security education, training, and awareness efforts throughout the DOE.

(14) Provides training information and material on DOE-wide cyber security threats, protection strategies, and organizational responsibilities.

b. Lead Program Secretarial Officers (LPSO).

(1) Coordinate with the CIO on 5a(5-7).

(2) Are responsible and accountable for cyber security of information resources under the purview of their respective programs.

(3) Ensure that adequate resources are budgeted and allocated to implement cyber security for their respective programs.

(4) Ensure that program roles and responsibilities for cyber security are clearly defined. The LPSO will ensure that a single, senior-level individual is designated as the focal point for cyber security in the headquarters, the field and operations offices, and each site as appropriate.

(5) Ensure that each DOE organization within their cognizance has an approved CSPP.

(6) Monitor the effectiveness of cyber security of unclassified National Security, Management and Administration, and Business Operations information through program reviews, self assessments, management assessments, performance metric results, and Independent Oversight evaluations; LPSOs may designate a representative to observe scheduled inspections and assessments conducted by Independent Oversight.

(7) Cooperate fully with external and internal review and oversight organizations, including Independent Oversight.

(8) In response to issues identified by Independent Oversight, develop corrective action plans within 60 days.

c. Line Managers Responsible for DOE Organization Cyber Security.[1]

(1) Assume responsibility and accountability for their organizations' cyber security programs.

(2) Ensure that adequate resources are allocated to the organization's Cyber Security Program.

(3) Ensure that organization roles and responsibilities for cyber security are clearly defined.

(4) Appoint a single individual responsible for all aspects of an organization's cyber security, such as an organization CIO or equivalent.

(5) Monitor the effectiveness of cyber security through self assessments and reviews.

(6) Assume responsibility for accepting residual risk.

(7) Cooperate fully with external and internal review and oversight organizations, including Independent Oversight.

(8) In response to issues identified by Independent Oversight, develop corrective action plans within 60 days.

d. Operations Office or Field Office Manager.

(1) Approves the organization CSPP.

(2) Shares responsibility for accepting residual risk when the DOE organization manager is a contractor.

e. The Office of Oversight and Performance Assurance (Independent Oversight).

(1) Designs and implements an independent oversight program that encompasses DOE cyber security policy and implementation of that policy at DOE organizations.

(2) As the sole focal point for DOE Headquarters oversight, periodically evaluates cyber security programs at DOE organizations. Such evaluations may include scheduled onsite inspections, unannounced inspections, remote scanning, penetration testing, and other such techniques.

[1] These individuals might be Laboratory directors, operations or field office managers, or responsible Headquarters managers.

(3) Develops inspection methods and tools for evaluating cyber security.

(4) Identifies and tracks issues identified during independent oversight activities.

(5) Recommends improvements for the Unclassified Cyber Security Program to the organizations, LPSOs, and CIO.

(6) Reviews selected Cyber Security Program Plans.

(7) Evaluates and rates the effectiveness or performance of DOE organizations in meeting the requirements and intent of cyber security policy.

(8) Solicits input from the CIO and Office of Counterintelligence on inspection topics of concern for scheduled inspections; notifies the CIO, Office of Counterintelligence, and LPSO of scheduled inspections and provides an opportunity to participate.

(9) Analyzes the effectiveness of and trends in Departmental cyber security.

(10) Cooperates with the CIO, LPSOs, DOE organization managers, and the Office of Counterintelligence to identify potential solutions to DOE-wide or high-priority DOE organization-specific problems, in a manner that does not compromise the independence of Independent Oversight.

f. DOE Computer Incident Advisory Capability (CIAC).

(1) Serves as the DOE central computer incident reporting and analysis capability.

(2) Assists DOE organizations as requested in dealing with incidents and in performing assistance reviews.

(3) Advises DOE organizations of cyber security incidents, threats, and vulnerabilities and provides a watch and warning capability for the Department.

(4) Analyzes incidents reported by organizations, prepares summary reports of the incident information, and provides these reports to line managers responsible for element cyber security, LPSOs, the CIO, and Independent Oversight.

g. Office of Counterintelligence.

(1) Coordinate with DOE elements, PSOs, the CIO and other policy and technical planning bodies in defining policy, identifying data and technical requirements, and implementing initiatives to meet CI needs and purposes.

(2) Conduct CI analysis of intrusion activity occurring across DOE sites.

(3) In coordination with CIO, OCI will coordinate the investigation of intrusions into the DOE systems with DOE field elements and NIPC until such time as it is determined that the intrusion is not a CI problem.

(4) OCI will perform independent inspections of CI programs at DOE facilities, to include evaluation of security components which impact the CI program, in coordination with Independent Oversight.

(5) In coordination with Independent Oversight, conduct vulnerability analyses and Red Teaming.

6. CONTACT. To provide comments and obtain assistance concerning this order, contact the Office of the Chief Information Officer at (202) 586-0166.

7. REFERENCES.

a. Clinger-Cohen Act of 1996. Public Law 104-106, which requires agencies to establish an information technology architecture.

b. National Technology Transfer and Advancement Act of 1995. Public Law 104-113, which supports Federal involvement in voluntary standards bodies.

c. Office of Management and Budget (OMB) Memorandum, June 18, 1997. A memorandum that concerns information technology architectures and calls for a technical reference model and standards profiles.

d. OMB Circular A-119. “Federal Participation in the Development and Use of Voluntary Standards.”

8. DEFINITIONS. Attachment 2 contains a listing of definitions specific to the DOE Unclassified Cyber Security Program.

BY ORDER OF THE SECRETARY OF ENERGY:

JOHN M. GILLIGAN
CHIEF INFORMATION OFFICER

CONTRACTOR REQUIREMENTS DOCUMENT

1. CYBER RESOURCE PROTECTION. Each DOE contractor must ensure that all DOE unclassified information and information systems under its purview are protected in a manner that is consistent with its threats and missions at all times.

2. RISK MANAGEMENT. Each DOE contractor must use a risk-based approach to protect information and information systems. A documented risk assessment process must be used to make informed decisions related to the adequacy of protection, cost implications of further enhanced protection, and acceptance of residual risk.

3. PROTECTION OF NON-DOE INFORMATION. Each DOE contractor must protect the information and information technology resources of other Federal Departments and agencies, State and local governments, and entities in the public sector.

4. CYBER SECURITY PROGRAM PLAN. Each DOE contractor must document its Cyber Security Protection Program in a Cyber Security Program Plan (CSPP). The CSPP must be approved by the DOE Office of the Chief Information Officer (CIO) and the Office of Independent Oversight and Performance Assurance (Independent Oversight). Contractors may revise their CSPPs as required by new operational considerations, risks, vulnerabilities, etc. Contractors must submit these revisions to their operations or field office manager. In urgent situations, they may anticipate approval and implement these revisions while waiting for formal approval.

5. CSPP ASSESSMENT AND REVIEW. To ensure that the CSPP is properly implemented, the contractor must ensure that the following three-level review process is used.

    a. Organization Self-Assessment. As called for by the CSPP, but no less frequently than once every 2 years, each DOE contractor must evaluate its conformance with the approved CSPP. The evaluation must include a threat and risk assessment and a vulnerability analysis of its information systems. The evaluation must also describe the residual risk accepted by the contractor, including a listing of any waivers from the policy mandated by either the CSPP or DOE.

    b. Peer Review. At least once every 3 years, a peer organization must evaluate each DOE contractor’s conformance with the approved CSPP. The results must be provided to the cognizant Federal line manager, DOE organization manager (e.g., lab director), operations/field office manager, and the Office of the CIO.

    c. Oversight Review. An oversight review must be performed on each DOE contractor’s Unclassified Cyber Security Program to assess its conformance with the approved CSPP.

These reviews will assess effectiveness of the cyber security protection program in meeting the requirements and intent of this directive and the contractor's CSPP. Independent Oversight will notify the DOE contractor, LPSO, CIO, Office of Counterintelligence, and the operations/field office manager of scheduled inspections, so they may participate. Results of each Independent Oversight review will be provided to the same individuals and may include ratings of program effectiveness and issues requiring development and implementation of corrective action plans.

6. CORRECTIVE ACTION PLANS. Each DOE contractor must draft and implement corrective action plans to address security shortfalls uncovered as a result of the oversight review process. The corrective action plans must include actions to be taken, responsible organizations and individuals for each action, schedule including key milestones, actions to address root causes and generic applicability, tracking of actions to closure, and steps to verify effectiveness of actions prior to closure.

7. THE SECURITY POLICY PLANNING GROUP. DOE contractors must provide representatives to this group as requested by DOE.

8. USER AUTHENTICATION. DOE contractors must employ user authentication techniques before allowing users to access systems that support multiple user accounts or systems that contain restricted, hard-to-replace, or sensitive data. The CSPP must indicate the systems or enclaves that require positive authentication and the type of authentication that must be employed.

9. ACCESS PROTECTION. Each DOE contractor must protect its information and information systems as specified in the CSPP. The CSPP must specify the information and systems to be protected and the protective mechanisms to be used.

10. AUDITING. Each DOE contractor must be capable of recording, and maintaining in an audit trail, information regarding access to and modifications of all information resources, where this is identified as appropriate by risk and vulnerability analysis, and such capability is technically feasible. The CSPP must state the systems or enclaves that must be audited, what information must be captured in that audit trail, and how long the audit trail must be maintained.

11. CONTINUITY OF SERVICE. DOE contractors must employ procedures and mechanisms to curtail or recover from activities that can disrupt or otherwise interfere with system availability, where operationally necessary and technically feasible. The CSPP must identify the contractor's systems and enclaves that require such mechanisms and procedures and must detail the procedures and mechanisms employed.

12. SECURITY MONITORING. Each DOE contractor must report security incidents to their site incident response team and to the Computer Incident Advisory Capability (CIAC). In addition, each DOE contractor must provide 24-hour-a-day, 7-day-a-week coverage. The CSPP must specify the type of events that require monitoring, the enclaves and systems that will be subject to monitoring, how the 24x7 monitoring will be handled, and the composition of the organization incident response team. DOE contractors must also provide security incident information to the National Infrastructure Protection Center (NIPC) and the DOE Office of Counterintelligence as necessary, in accordance with all agreements.

13. CYBER SECURITY ADVISORIES, ALERTS, AND SUSPECTED INCIDENTS. Contractor personnel must respond to CIAC cyber security advisories, bulletins, alerts, and suspected incidents in accordance with the policy and procedures stated in the organization's CSPP. The specific response must be commensurate with the perceived level of risk and may include containment, remediation, and increased monitoring.

14. TRAINING. All DOE contractor personnel must be appropriately trained in cyber security vulnerabilities, threats, protection strategies, and respective organizational and personal responsibilities. The CSPP must specify the details of the training program.

15. MALICIOUS CODE. Each DOE contractor must establish procedures and mechanisms, consistent with the threat environment, to limit (as technically feasible) the introduction of malicious code into its information systems. The CSPP must specify the mechanisms used to detect and prevent the installation of malicious code and the frequency of updating such mechanisms.

16. MISSION INTEROPERABILITY CLUSTERS. To facilitate consistency of security implementation among the DOE organizations, five specific mission interoperability clusters have been defined. In its CSPP, the contractor must specify the mission interoperability clusters applicable to its mission and environment.

17. CSPP CONTENTS. The CSPP for each DOE contractor must detail the approach to ensuring effective cyber security. The CSPP must account for the contractor's specific environment, missions, and threats. At a minimum, the CSPP must address the following aspects of security.

    a. Define and assign cyber security roles and responsibilities.

    b. Define and describe cyber boundaries and boundary protection techniques, including the scope, specific security policies, connections external to an organization or identified enclave, and protection mechanisms required.

c. Describe configuration management policies and practices, including a description of the process for making significant changes to the information system architecture and the contractor organization's definition of "significant changes."

d. Describe the procedures for responding to incidents at the organization, enclave, or system level as appropriate and in coordination with the Computer Incident Advisory Capability.

e. Describe the type of changes in technology, threat environment, or other changes to the organization, enclave, or system environment and architecture that would require the CSPP to be updated prior to its normal 2-year cycle.

f. Describe the cyber security controls (technical and non-technical) employed to ensure confidentiality, integrity, availability, and accountability as required to accommodate the specific threats identified for information entered, processed, stored, displayed, or transmitted. These include, but are not limited to, the following:

(1) Authentication: Describe the type of authentication mechanisms employed, identify the systems and enclaves that require positive authentication, and, for those systems and enclaves that do not require positive user authentication, provide a rationale for said decisions.

(2) Access Protection: Describe the access control process and procedure employed at the DOE organization, which include, but are not limited to–

(a) identification of those information systems that require isolation or protection;

(b) summary of strategy for securely accessing enclaves from locations outside of the enclave (including locations both inside and outside of the DOE organization); and

(c) a description of circumstances under which penetration testing may be used to validate access protection mechanisms.

(3) Audit: Specify the enclaves, systems, and services (including email) that will be subject to auditing, what information must be collected, and how long audit information must be maintained.

(4) Security Monitoring: Describe the type of events for which monitoring must be employed, which enclaves, clusters, and systems are subject to monitoring, and how 24x7 monitoring will be handled.

(5) Denial of Service: Identify those enclaves and systems that, due to mission operation necessities, have a low tolerance for disruption or unavailability; describe the procedures and mechanisms that will be employed to limit (as technically feasible) and recover from such disruption or unavailability.

g. Describe the process for ascertaining the current operational threat, risk, and vulnerability posture; the description must specify–

(1) who (by title/position) within the organization conducts the threat, risk, and vulnerability assessments;

(2) how such threat, risk, and vulnerability assessments are to be conducted; and

(3) how frequently such assessments must be conducted.

h. Describe the methodology being used for training (e.g., briefings, email), specify how frequently re-training should occur, identify those positions requiring training, and identify (by title/position) those responsible for overseeing training activities at the contractor's organization.

i. Describe the approach employed to address malicious code (e.g., handled at boundary, handled at desktops, handled at selected locations), the mechanisms employed, and frequency of updating anti-malicious code software.

j. Describe the metrics employed to assess compliance with the CSPP and the process for evolving these metrics.

k. Describe the process for selecting peer members to review the contractor's CSPP and its compliance with the CSPP. The description should include qualifications required of the prospective individuals or entities and who makes the selection.

l. Identify those mission interoperability clusters that are applicable to the DOE contractor's organization.

m. Identify (by title/position) the DOE contractor's organization manager.

DEFINITIONS

The following terms are specific to the DOE Unclassified Cyber Security Program. Some definitions include a citation indicating the source. Citations are given in full on first use and are abbreviated thereafter. Where no citation appears, the term has been derived from several sources or from common usage. Many definitions are from the National Security Telecommunications and Information Systems Security Committee's *National Information Systems Security (INFOSEC) Glossary*. Other definitions may be found in the *DOE Glossary*, which is available online.

ACADEMIC RESEARCH/SCIENCE OPERATIONS. The mission interoperability cluster dealing with information used for academic research and for operating science facilities.

AUDIT TRAIL. A chronological record of system activities that is sufficient to enable the reconstruction, reviewing, and examination of the sequence of environments and activities surrounding or leading to an operation, a procedure, or an event in a transaction from its inception to final results. [National Computer Security Center, *Glossary of Computer Security Terms*, 21 October 1988.]

AUTHENTICATION. Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information. [National Security Telecommunications and Information Systems Security Committee. *National Information Systems Security (INFOSEC) Glossary*. NSTISSI No. 4009, August 1997. Hereafter cited as "NSTISSI 4009."]

COMPUTER INCIDENT ADVISORY CAPABILITY (CIAC). The Department-wide computer network incident response capability; a dedicated capability to monitor, analyze, track, summarize, and report cyber security incidents, and to issue alerts and advisories.

COMPUTER NETWORK. An interconnected collection of autonomous computers. [DOE Glossary]

CONFIGURATION MANAGEMENT. Management of security features and assurances through control of changes made to hardware, software, firmware, documentation, test, test fixtures, and test documentation throughout the life cycle of an information system. [NSTISSI 4009.]

CONTAINMENT. Ensuring that neither attacks nor responses result in severe and undesirable damage, either to operational capabilities, to any personnel, or to equipment or property of any kind.

CONTRACTOR. See DOE contractor.

COUNTERMEASURE. Anything that effectively negates an intruder's ability to exploit vulnerabilities.

CYBER SECURITY. The protection of information systems against unauthorized access to or modification of information, whether in storage, processing, or transit, against loss of accountability for information and user actions, and against the denial of service to authorized users, including those measures necessary to protect against, detect, and counter such threats.

DENIAL OF SERVICE. Result of any action or series of actions that prevents any part of an information system from functioning. [NSTISSI 4009.]

DEPARTMENTAL ELEMENTS. First-tier organizations at Headquarters and in the field. First-tier entities at Headquarters are the Secretary, Deputy Secretary, Under Secretary, and Secretarial Officers (Assistant Secretaries and Staff Office Directors). First-tier entities in the field are Managers of the eight operations offices, managers of the three field offices, and the administrators of the power marketing administrations. Headquarters and field elements are described as follows:

1. Headquarters elements are DOE organizations located in the Washington metropolitan area.

2. “Field elements” is a general term for all DOE elements (excluding individual duty stations) located outside of the Washington, DC, metropolitan area. [DOE Glossary]

DOE CONTRACTOR. An entity who receives an award from DOE, including management and operating contractors, which manage, operate, or provide DOE element services to DOE research or production facilities that are principally engaged in work for the DOE. [DOE Glossary]

DOE ORGANIZATION. A Department Headquarters element or field element that includes both DOE Federal and DOE contractor entities.

DOE ORGANIZATION MANAGER. The Federal employee or contractor who heads a DOE organization.

ENCLAVE. A set of information and processing capabilities that are protected as a group.

EXPORT CONTROLLED INFORMATION. Certain unclassified Federal Government information under DOE’s cognizance that, if generated by the private sector, would require a specific license or authorization for export under U.S. laws or regulations. [DOE Glossary]

FIELD ELEMENT. See Departmental element. [DOE Glossary]

GOVERNMENT INFORMATION. Information created, collected, processed, disseminated, or disposed of by or for the Federal Government. [DOE Glossary]

INCIDENT. Any adverse event that threatens the security of information resources. Adverse events include compromises of integrity, denial of service, compromises of confidentiality, loss of accountability, or damage to any part of the system. Examples of incidents include the insertion of malicious code (e.g., viruses, Trojan horses, or backdoors), unauthorized scans or probes, successful and unsuccessful intrusions, and insider attacks.

INDUSTRY/OTHER (NON-NATIONAL SECURITY/ACADEMIC) GOVERNMENT RESEARCH. The mission interoperability cluster dealing with information and functions, such as Cooperative Research and Development Agreements (CRADAs), "work for others," proprietary information trade agreements, and industrial/commercial collaborative research.

INFORMATION. Any communication or reception of knowledge such as facts, data, or opinions including textual, numerical, graphic, cartographic, narrative, or audiovisual forms, whether oral or maintained in any medium, including computerized databases, paper, microform, or magnetic tape. [DOE Glossary]

INFORMATION RESOURCES. Information, information technology, and information systems.

INFORMATION SYSTEM. A discrete set of information and information technology organized to collect, process, maintain, transmit, and disseminate information, in accordance with defined procedures, whether automated or manual.

INTEROPERABILITY. The ability of systems, units, or forces to provide services to and accept services from other systems, units, or forces and use the services so exchanged to enable them to operate together. [DOE Glossary]

INTEROPERABILITY STANDARD. A document that establishes engineering and technical requirements necessary to be employed in the design of systems, units, or forces and to use the services so exchanged to enable them to operate effectively together. [DOE Glossary]

INTRUSION. An unauthorized access to an information resource.

INTRUSION DETECTION. The logging and auditing capability that provides evidence that an attempt or actual breach of protection mechanisms or access controls has occurred.

LEAD PROGRAM SECRETARIAL OFFICER. See secretarial officer.

MAJOR APPLICATION. An application that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. Note; All Federal applications require some level of protection. Certain applications, because of the information in them; however, require special management oversight and should be treated as major. Adequate security for other applications should be provided by security of the systems in which they operate. (Source: Appendix III to OMB Cicular No. A-130)

MANAGEMENT/ADMINISTRATIVE/BUSINESS OPERATIONS. The mission interoperability cluster that deals with such functions as personal dosimetry reports, contractor performance appraisals (including fees and penalties data), personnel data, other-than-science facility operations, production operations, grants and proposal administration, and procurement data. DOE contractor systems that are incidental to the contract in this cluster are the sole responsibility of the contractor.
MISSION INTEROPERABILITY CLUSTER (MIC). Information resources performing similar functions within DOE that use data of similar sensitivity levels, and that have similar computer security concerns and protection requirements across all DOE organizations.

The five specific mission interoperability clusters are listed below.

1. Unclassified National Security/Nuclear: Information that is unclassified but still requires protection, such as Unclassified Controlled Nuclear Information (UCNI), export-controlled information (ECI), and Naval Nuclear Propulsion Information (NNPI).

2. Management, Administration, Business Operations: Information that is unclassified but still requires protection, such as proprietary information (but not third-party proprietary), Privacy Act, and the majority of the exemptions to the Freedom of Information Act ("Official Use Only" information).

3. Industry and Other Government Research: Information that is unclassified but still requires protection, such as third-party proprietary information, Protected CRADA (Cooperative Research and Development Agreement) Information, and other information protected by its sponsor (such as "technical data" from the Department of Defense).

4. Academic Research, Scientific Operations: Information that is unclassified but is considered sensitive because it is in "pre-publication" form and is not appropriate for general release; it may or may not require special protection.

5. Open, Public, Unrestricted: Information that requires no protection from disclosure.

MONITORING. Near-real-time collection and analysis of information about system behavior, such as throughput or performance, which could indicate a security incident.

OFFICIAL USE ONLY.

1. A designation identifying certain unclassified but sensitive information that may be exempt from public release under the Freedom of Information Act or

2. a former (7-18-49 through 10-22-51) security classification marking. [DOE Glossary]

OPEN/PUBLIC/UNRESTRICTED. The mission interoperability cluster dealing with information provided for public access.

OVERSIGHT. Refers to the responsibility and authority assigned to the Assistant Secretary for Environment, Safety and Health to independently assess the adequacy of DOE and contractor performance. Oversight is separate and distinct from line management activities, including self-assessments. [DOE Glossary]

PERFORMANCE MEASURE. A process of assessing progress toward achieving predetermined goals. [DOE Glossary]

PROGRAM OFFICE. A Headquarters organization that is responsible for executing program management functions, and which is responsible for assisting and supporting field elements in safety and health, administrative, management, and technical areas. [DOE Glossary]

PROGRAM SECRETARIAL OFFICER. See secretarial officer. [DOE Glossary]

REMEDIATION. Recovery of functional capabilities; restoration of the integrity of data and software; removal of malicious code, data, and devices; and repair of physical damage.

RESEARCH. A systematic investigation, including research, development, testing, and evaluation, designed to develop or contribute to general knowledge. Activities that meet this definition constitute "research" for purposes of protecting human subjects, whether or not they are conducted under a program considered research for other purposes (i.e., some "demonstration" and "service" programs may include research activities). [DOE Glossary]

RESPONSIVE ACTIVITIES. Activities taken in response to a cyber security advisory, alert, or suspected incident, including containment, reporting, monitoring and observation, remediation, retaliation (e.g., legal action), and presentation of information to the public or to other organizations.

RESIDUAL RISK. The portion of risk remaining after security measures have been applied. [NSTISSI 4009.]

RISK. The probability that an undesired result or event such as theft, loss, damage, or injury will occur. Exposure to the chance of loss, damage, or injury. [DOE Glossary]

SAFEGUARDS AND SECURITY INTEREST. A general term for any DOE asset, resource, or property that requires protection from malevolent acts. It may include but is not limited to classified matter, special nuclear material and other nuclear materials, secure communications centers, sensitive compartmented information facilities, automated data processing centers, facilities storing and transmitting classified information, vital equipment, or other DOE property. [DOE Glossary]

SECRETARIAL OFFICER. Secretarial Officers are the Secretary, Deputy Secretary, and Under Secretary; and the Assistant Secretaries and Staff Office Directors reporting to the Secretary either directly or through the Deputy Secretary or Under Secretary. The following designations are also used to identify Secretarial Officers with specific responsibilities in various areas.

1. A Program Secretarial Officer is a Head of a Departmental element who has responsibility for a specific program or facility(ies). These include the Assistant Secretaries for Defense Programs, Energy Efficiency and Renewable Energy, Environmental Management, and Fossil Energy; and the Directors of the Offices of Civilian Radioactive Waste Management, Science, and Nuclear Energy.

2. A Cognizant Secretarial Officer is a DOE official at the Assistant Secretary level who is responsible for the assignment of work, the institutional overview of any type of facility, or both, and the management oversight of a laboratory. [DOE Glossary]

THREAT. Any circumstance or event with the potential to cause harm to an information system in the form of destruction, disclosure, adverse modification of data, and/or denial of service. [NSTISSI 4009.]

TRAINING. The process of providing for and making available to an employee(s) and placing or enrolling an employee(s) in a planned, prepared, and coordinated program, course, curriculum, subject, system, or routine of instruction or education, in fiscal, administrative, management, individual development, or other fields that improve individual and organizational performance and assist in achieving the agency's mission and performance goals. [DOE Glossary]

UNCLASSIFIED. The designation for information, a document, or material that has been determined not to be classified or that has been declassified by proper authority. [DOE Glossary]

UNCLASSIFIED NATIONAL SECURITY/NUCLEAR. The mission interoperability cluster dealing with unclassified information and systems related to national security. This MIC includes the following systems: Unclassified Controlled Nuclear Information (UCNI), Naval Nuclear Propulsion Information (NNPI), military/dual use information, nonproliferation information, and other sensitive, but not classified, information.

USER AUTHENTICATION. Reliable identification of users of an information system.

VIRUS. Self-replicating, malicious program segment that attaches itself to an application program or other executable system component and leaves no obvious signs of its presence. [NSTISSI 4009.]

VULNERABILITY. A weakness or system susceptibility that if exploited would cause an undesired result or event leading to loss or damage, as follows:

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

2. Unspecified Major Vulnerability is a major vulnerability, but specified in no greater detail than the specific security system (or one of its major components) when it occurs. A weakness in a system or organization's defenses that could be exploited. [DOE Glossary]

VULNERABILITY ANALYSIS. A systematic evaluation process in which qualitative and/or quantitative techniques are applied to detect vulnerabilities and to arrive at an effectiveness level for a safeguards and security system to protect specific targets from specific adversaries and their acts. [DOE Glossary]

VULNERABILITY ASSESSMENT. See vulnerability analysis.