Information System Security Critical Elements

Please note that prior to including this language in the performance plans of employees covered by bargaining units, all labor relations obligations must have been fulfilled.

Stand-Alone Critical Elements

Senior Agency Information Security Officer/Chief Information Security Officer/ Information Technology Security Officer

Critical Element and Objective

- Senior Agency Information Security Officer/Chief Information Security Officer/ Information Technology Security Officer
- To manage the information and IT security program.

Required Results/Results of Major Activities

- IT security continuous monitoring process is managed.
- Incident response capability is managed.
- Authorization process is managed.
- Information security requirements are developed, disseminated and maintained.
- General awareness and security role-based training is coordinated and provided.

Evaluation Criteria *(for Two-Level employees, on the CD-516, select "Other" under the appropriate Performance Indicator and insert the language below)*

- IT security continuous monitoring process is completed at a minimum annually.
- Incidents are identified and responded to in accordance with reporting categories and deadlines outlined in the IT Security Program Policy.
- Authorization process is managed and completed in accordance with the IT Security Program Policy and operating unit procedures.
- Information security requirements are developed, disseminated and maintained in accordance with DOC and Federal policies and requirements.
- Changes to security requirements are generally communicated in a timely manner to CIO/AO/ISO/ISSO.
- General awareness and role-based training is usually provided to employees on an annual basis and tracked in accordance with Departmental and operating unit requirements.

Information System Security Officer (ISSO)

Critical Element and Objective

- Information System Security Officer (ISSO)
- To implement and manage systems' information and IT security controls of systems.

Required Results/Results of Major Activities

- Changes to information system are controlled and managed.
- Information and IT security controls are implemented and monitored.
- Authorization documentation and related artifacts are created and maintained.
- Changes to security requirements are coordinated and disseminated.

Evaluation Criteria *(for Two-Level employees, on the CD-516, select "Other" under the appropriate Performance Indicator and insert the language below)*

- Plans of actions and milestones (POAMs) are accurately identified; development and resolution of a timeline meets the system owner's expectations and is entered into the DOC Cyber Security Assessment and Management (CSAM) tool in a timely manner.
- Information and IT security controls are implemented and assessed in accordance with DOC's Continuous Monitoring Plan and the DOC IT Security Program Policy.
- Authorization documentation and related artifacts are created and maintained in accordance with IT Security Program Policy.
- Changes to security requirements are usually communicated in a timely manner to ISO and SAISO/CISO/ITSO.

Collateral Duties – Critical Element Language May be Incorporated into Existing Element

Information System Owner (ISO)

Required Results/Results of Major Activities

- System security authorization documentation is developed and maintained.
- System security controls are implemented and monitored.

Evaluation Criteria *(for Two-Level employees, on the CD-516, select "Other" under the appropriate Performance Indicator and insert the language below)*

- Documentation is an accurate description of implemented system security controls, in accordance with the DOC IT Security Program Policy, and usually updated in a timely manner.

- System security controls are implemented and monitored in accordance with the operating procedures as defined in the authorization document.

Certification Agent (CA)

Required Results/Results of Major Activities

- Assessment of information system undergoing authorization is completed and vulnerabilities are identified.

Evaluation Criteria *(for Two-Level employees, on the CD-516, select "Other" under the appropriate Performance Indicator and insert the language below)*

- The Security Assessment Report is typically well researched, includes an assessment of the security controls, is completed within 60 days of assessment, and is in accordance with IT Security Program Policy and operating unit procedures.

Incident Response Personnel (IR)

Required Results/Results of Major Activities

- Information technology security events or incidents are addressed.

Evaluation Criteria *(for Two-Level employees, on the CD-516, select "Other" under the appropriate Performance Indicator and insert the language below)*

- Remedial actions in response to information technology security events or incidents are generally coordinated and reported in accordance with operating unit procedures.

Key Contingency Roles

Required Results/Results of Major Activities

- Contingency/Disaster Recovery/COOP Plans and activities are coordinated, documented, maintained and tested.

Evaluation Criteria *(for Two-Level employees, on the CD-516, select "Other" under the appropriate Performance Indicator and insert the language below)*

- Contingency/Disaster Recovery/COOP plans and activities are accurately documented and maintained, tested annually, and coordinated in a timely manner with AO/ISO/ITSO/SAISO/ISSO/DR and/or COOP coordinator.