INTELLIGENCE COMMUNITY STANDARD

502-01

20 December 2013

# Intelligence Community Computer Incident Response and Computer Network Defense

**A. AUTHORITY:** The National Security Act of 1947, as amended; Executive Order 12333, *United States Intelligence Activities*, as amended; Intelligence Community Directive (ICD) 500, *Director of National Intelligence Chief Information Officer*; ICD 502, *Integrated Defense of the Intelligence Community Information Environment*; and other applicable provisions of law.

**B. PURPOSE:** This Intelligence Community Standard (ICS) defines the baseline computer incident response responsibilities, capabilities, and supporting computer network defense (CND) services that Intelligence Community (IC) elements and IC Information Technology Enterprise (ITE) Service Providers shall establish and maintain, on a 24 hours per day, seven days per week basis, within their respective enterprises. This ICS supports the implementation of ICD 502 and the execution of the *Concept of Operations for the Integrated Defense of the IC Information Environment*.

**C. APPLICABILITY**

1. This Standard applies to the IC, as defined by the National Security Act of 1947, as amended, and such other elements of any other department or agency as may be designated by the President, or designated jointly by the Director of National Intelligence (DNI) and the head of the department or agency concerned, as an element of the IC.

2. This standard applies to the IC Information Environment (IE) which is defined as all individuals, organizations and information technology (IT) capabilities that collect, process or share Sensitive Compartmented Information, or that regardless of classification, are operated by the IC and are wholly or majority National Intelligence Program (NIP) funded. The IC IE is an interconnected shared risk environment where the risk accepted by one IC element is effectively accepted by all IC elements.

3. This Standard also applies to the IC ITE as the strategic implementation of the IC IE, to include enterprise services.

**D. IMPLEMENTATION**

1. IC elements will implement and maintain the following minimum baseline CND services and capabilities based on the *Concept of Operations for the Integrated Defense of the IC Information Environment*: incident monitoring, response and reporting; vulnerability management; vulnerability scanning and assessments; threat assessments; and network security evaluations.

2. IC elements may implement more stringent requirements than those of this Standard as necessary to support their respective missions and internal security requirements to the extent that it will not inhibit situational awareness and information sharing.

3. If an IC element cannot support a requirement of this Standard, a waiver may be granted for implementing the requirement.

a. For IC ITE services of common concern and systems in the shared environment, all waivers from the requirements in this Standard shall be submitted to the IC CIO for review and approval. To ensure timely consideration, waiver requests shall identify the specific implementation requirements at issue and, as appropriate, state the cost, schedule, operational performance, and information security impacts that would be incurred without the waiver. Waiver requests, as appropriate, shall also describe a transition plan for eventual compliance with the specific requirements at issue. The IC CIO will respond to all waiver requests within 30 business days of the date of submittal.

b. For informational purposes, all non-ITE systems systems in the IC IE which do not meet the requirements of this ICS, shall report discrepancies to the IC CIO and, as appropriate, state the cost, schedule, operational performance, and information security impacts that would be incurred in order to achieve full compliance.

4. Participating organizations may elect to implement some of the capabilities of this Standard through subscriber-based service agreements with other IC elements. When subscribing services from another organization, the subscriber must ensure that the provider has agreed in a formal Service Level Agreement (SLA) to implement the requirements in this Standard.

## E. RESPONSIBILITIES

1. IC elements shall:

a. When designated as providing services of common concern, implement this Standard on behalf of subscribed, serviced, and supported IC elements and organizations.

b. Establish and maintain a 24 hours per day, seven days per week CND capability to implement and execute incident monitoring, incident reporting, and incident handling as defined in this Standard. An IC element's CND capability will provide a primary conduit for reporting to and interacting with the IC Incident Response Center (IC-IRC) on CND operations.

c. Establish collaboration and information sharing processes for implementing incident response and CND activities that include, as applicable, the following IC element organizations: personnel security, counterintelligence, law enforcement, management, information security, IT support, legal, privacy, inspector general, public affairs, and facilities management.

d. Implement the following capabilities specific to incident monitoring, response, and reporting activities:

(1) Develop, disseminate, review, and update annually a formal documented incident response policy, plan, and corresponding implementation procedural document that addresses purpose, scope, roles, responsibilities, coordination among element organizational entities, and compliance with documented incident response policy.

(2) Train all IC IE user personnel annually on their incident response roles and responsibilities, and require personnel to report suspected incidents.

(3) Internally test and/or exercise the incident response capabilities and training capabilities at least annually including using simulated operational incidents, and participate with other IC elements in IC-wide CND operational exercises.

(4) Implement incident response, incident handling tools and procedures that include: preparation, detection, analysis, containment, eradication, and recovery; employ automated mechanisms to support the incident handling process; incorporate lessons-learned from incident handling events into incident response procedures, training, and testing/exercises; and identify classes of incidents and define ranges of approach response actions to ensure the continuation of the mission and operational intelligence functions. Handling procedures shall include counterintelligence and law enforcement entities for attribution, forensics, and evidence chain of custody when appropriate.

(5) Monitor users, networks, vulnerabilities, and infrastructure (in real-time or near real-time) to detect, respond, track, and document incidents occurring within the IC IE. Employ automated mechanisms to assist in the tracking of incidents and in the collection and analysis of incident information.

(6) Maintain a capability to respond to IC-IRC action orders, advisories, Integrated Defense Management Teams (IDMT) stand-ups, and other IC-wide courses of action as defined in the *Concept of Operations for the Integrated Defense of the IC Information Environment*.

(7) Develop and maintain internal processes for elevating reports on information system weaknesses, deficiencies, and/or vulnerabilities associated with reported incidents to the IC element senior leadership and IC element stakeholders.

(8) Report incident information to the IC-IRC in accordance with the *Intelligence Community Incident Reporting Procedures*, or subsequent guidance. Provide additional incident information to the IC-IRC, as requested.

(9) Notify the IC-IRC of any significant organizational changes that may positively or negatively impact the ability or capability of the IC element to report, defend, and operate its part of the IC IE.

(10) Establish and maintain the capability to conduct forensic services and malware analysis, participate in the IC Coordinated Response Process (CRP), respond to requests for information from the IC-IRC and other IC element CND centers, and request support, when necessary, from IC-IRC and other IC element CND centers.

e. Implement the following capabilities specific to vulnerability management:

(1) Acknowledge receipt and comply with IC-IRC issued IC vulnerability alerts, messages, and warnings within the timeframe designated by the IC-IRC. Report compliance to IC-IRC in accordance with IC-IRC vulnerability management procedures. If unable to meet the compliance deadline, provide the IC-IRC with an anticipated compliance date and vulnerability mitigation strategy.

(2) Report to the IC-IRC any discovered vulnerabilities with potential impacts to IC IE networks and systems.

(3) Generate internal security alerts, advisories, and directives, as necessary, and disseminate among IC element stakeholders, customers, and IC IE users.

(4) Create and maintain an inventory of IT resources, including hardware, operating systems, and software applications, used within the IC element or maintained by the element as a shared resource, that can be used to assess the IC element's exposure and potential impact to vulnerabilities.

(5) Develop a vulnerability management plan and update this plan annually as necessary.

f. Implement the following capabilities specific to vulnerability scanning and assessments:

(1) Conduct vulnerability assessments and perform enterprise scans for known vulnerabilities, patch assessment, and configuration compliance. A full comprehensive scan shall be conducted at least annually.

(2) Employ vulnerability scanning tools and techniques that promote interoperability in the IC IE and that automate parts of the IC IE vulnerability management processes by using standards for: enumerating platforms, software flaws, and improper configurations; formatting and making transparent, checklists and test procedures; and measuring vulnerability impact.

(3) Incorporate the discovery of vulnerabilities into the IC element's Risk Management Framework for mitigation.

(4) Report vulnerability scanning and assessment information, status, and results to element leadership and IC IE stakeholders consistent with processes as outlined in the *Concept of Operations for the Integrated Defense of the IC Information Environment*. Report compliance of an annual vulnerability assessment, executive level summary of vulnerability status, and results to the IC-IRC and share results with other IC element organizations.

g. Implement the following capabilities specific to threat assessments:

(1) Conduct threat assessments to identify and evaluate threats to enterprise information systems, networks, and shared IC resources. The threat assessment should include a malicious actor's intent, capabilities, and potential targets. A threat assessment shall be conducted at least annually.

(2) Incorporate discovered threat information into the IC element's Risk Management Framework for mitigation.

(3) Report threat assessment information, status, and results to IC element leadership and IC stakeholders. Report compliance of an annual threat assessment and executive level summarized results to the IC-IRC and share results with other IC element organizations.

h. Implement the following capabilities specific to network security evaluations:

(1) Conduct network security evaluations (Red or Blue Team). An adversary perspective evaluation must be conducted at least once every two years.

(2) Incorporate the discovery of vulnerabilities into the IC element's Risk Management Framework for mitigation.

(3) Report network security evaluation information, status, and results to IC element leadership and IC IE stakeholders consistent with processes as outlined in the *Concept of Operations for the Integrated Defense of the IC Information Environment*. Report compliance of

an annual network security evaluation and executive level summarized results to the IC-IRC and share results with other IC element organizations.

i. Analyze and correlate vulnerability assessments, threat assessment, and network security evaluation results from identified baseline security protections and controls to identify shortcomings in the IC element's defense portfolio.

j. Collaborate with the IC-IRC and other IC elements on signature and indicators development for specific threats and vulnerabilities to the IC IE, contribute signatures and indicators of interest, and incorporate signatures and indicators of interest into IC element detection and sensor technologies.

**F. EFFECTIVE DATE:** This Standard becomes effective on the date of signature.

Al Tarasiuk

Al Tarasiuk
Assistant Director of National Intelligence and
Intelligence Community Chief Information Officer

12/23/2013

Date

## Appendix A - References

1. Committee on National Security Systems (CNSS) Instruction 4009, *A Common Information Assurance Glossary for National Security Systems*, (April 2010).

2. Intelligence Community Chief Information Officer, *Concept of Operations for the Integrated Defense of the IC Information Environment*, (September 30, 2011).

3. Intelligence Community Chief Information Officer, *Intelligence Community Incident Reporting Procedures*, (September 21, 2011).

4. Intelligence Community Directive 500, *Director of National Intelligence Chief Information Officer*, (August 7, 2008).

5. Intelligence Community Directive 502, *Integrated Defense of the Intelligence Community Information Environment*, (March 11, 2011).

6. Intelligence Community Directive 503, *Intelligence Community Information Technology Systems Security Risk Management, Certification and Accreditation*, (September 15, 2008)

## Appendix B – Terms and Definitions

Computer Network Defense (CND): Actions taken to defend against unauthorized activity within computer networks. CND includes monitoring, detection, analysis (such as trend and pattern analysis), and response and restoration activities.

CND Service: A service provided or subscribed to by owners of IC information systems or computer networks to maintain and provide CND situational awareness; implement CND protect measures; monitor and analyze in order to detect unauthorized activity; and implement CND operational direction.

Coordinated Response Process (CRP): A structured methodology for executing an integrated defense response to a cyber situation (i.e., incident, vulnerability, threat or other event) affecting the IC IE, or having the potential to impact the IC IE. This process describes how the IC will respond to a significant cyber situation through the situation's life cycle from steady state, through response and recovery, and back to steady state. Details can be found in the *Concept of Operations for the Integrated Defense of the IC Information Environment.*

Enterprise: An organization with a defined mission/goal and a defined boundary, using information systems to execute that mission, and with responsibility for managing its own risks and performance. An enterprise may consist of all or some of the following business aspects: acquisition, program management, financial management (e.g., budgets), human resources, security, and information systems, information and mission management.

Incident: An assessed occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system; or the information the system processes, stores, or transmits; or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

Incident Monitoring: The active process of sensing information or information systems for an indication or occurrence of an incident.

Incident Response: The mitigation of violations of security policies and recommended practices.

Incident Response Plan: The documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of an incident against an organization's IT systems(s).

Indicator: Recognized action, specific, generalized, or theoretical, that an adversary might be expected to take in preparation for an attack.

Information System: A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

Integrated Defense Management Team (IDMT): A temporary group established by the IC CIO to address a significant cyber incident or event affecting or impacting the IC IE. The IDMT is instrumental in the Coordinated Response Process. Details can be found in the *Concept of Operations for the Integrated Defense of the IC Information Environment.*

IC Element: The agencies and departments that comprise the IC.

IC Information Environment: The individuals, organizations, and information technology capabilities that collect, process, or share Sensitive Compartmented Information, or that regardless of classification, are operated by the IC and are wholly or majority National Intelligence Program-funded.

IC Information Technology Enterprise (ITE): The strategic implementation of the IC information environment to enable greater IC integration, information sharing and safeguarding through a new common IC information technology architecture that substantially reduces costs.

ITE Service Provider: IC element organization specified to provide resources and services for the shared and unshared ITE.

Network Security Evaluation: Network security evaluations are comprehensive examinations of a network, its architecture, and its defenses. The objectives of network security evaluations are to: identify vulnerabilities in operational systems, measure the effectiveness of security policy and effect changes, and demonstrate the impact of network vulnerabilities when attacked. Network security evaluations expand upon basic vulnerability scanning by utilizing a combination of trained personnel, custom tools, and social engineering techniques to evaluate security controls. There are two forms of network security evaluations: an adversary perspective evaluation ("Red Team") and a cooperative/collaborative evaluation ("Blue Team").

Risk Management Framework: A structured approach used to oversee and manage risk for an enterprise.

Service Level Agreement (SLA): Defines the specific responsibilities of the service provider and sets the customer expectations.

Service Provider: IC element organization responsible for delivering CND protection, detection, and response services on a subscription basis to another IC element.

Signature: A characteristic byte pattern used in malicious code or an indicator, or set of indicators that allows the identification of malicious network activities.

Threat Assessment: Process of formally evaluating the degree of threat to an information system or enterprise and describing the nature of the threat.

Vulnerability: Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source.

Vulnerability Assessment: Systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.

Vulnerability Scanning: Utilization of a computer program/process to conduct vulnerability assessments.