National Geospatial-Intelligence Agency

DIRECTIVE

NUMBER 8231
19 May 2015
Administrative Update 4, 28 October 2015

~~T~~/CIO-*T*

SUBJECT: Cyber Defense Operations

References: See Enclosure 1.

1. PURPOSE. This NGA Directive (NGAD):

a. Establishes policy and assigns responsibilities for centralized NGA cyber defense operations.

b. Supports the national Intelligence Community (IC) and Department of Defense (DoD) cyber defense operations objectives in accordance with (IAW) References (a), (b), and (d) through (i).

c. Establishes the Cyber Security Operations Cell (CSOC) as the central point for all NGA cyber defense operations.

d. Supports cyber defense operations interoperability between agencies, combatant commands, and services.

2. APPLICABILITY. This NGAD applies to NGA civilian employees, military service members assigned to the NGA, personnel from other Government agencies permanently assigned to NGA, and contractors.

3. DEFINITIONS. See Glossary.

4. POLICY. It is NGA policy that:

a. All NGA cyber defense operations are consolidated and centralized under the CSOC, which serves as the focal point for NGA's cyber incident detection, analysis, and reporting and is the Computer Network Defense-Service Provider (CND-SP) for NGA networks and information systems (ISs).

b. The NGA CND-SP is certified and accredited IAW Reference (h).

c. Technical and non-technical capabilities are employed to implement directed information network operations and cyberspace defense actions to protect NGA networks and ISs IAW Reference (f).

5. RESPONSIBILITIES. See Enclosure 2.

6. EFFECTIVE DATE. This Directive is effective on the date of signature.

Harry E. Mornston
Chief of Staff

Enclosures
1. References
2. Responsibilities

Glossary

ENCLOSURE 1

REFERENCES

(a) Intelligence Community Directive (ICD) 502, "Integrated Defense of the Intelligence Community Information Environment," 11 March 2011
(b) ICD 503, "Intelligence Community Information Technology Systems Security Risk Management, Certification and Accreditation," 15 September 2008
(c) Committee on National Security Systems Instruction (CNSSI) 4009, "Committee on National Security Systems Glossary," *06* April ~~6,~~ 2015
(d) DoD Instruction (DoDI) 8500.01, "Cybersecurity," 14 March 2014
(e) DoD 8570.01-M, Information Assurance Workforce Improvement Program," 19 December 2005 (Incorporating Change 3, 24 January 2012)
(f) DoDI 8410.02, "NetOps for the Global Information Grid (GIG)," 19 December 2008
(g) DoD O-8530.1, "Computer Network Defense (CND)," *0*8 January 2001
(h) DoD O-8530.01-M, "Department of Defense Computer Network Defense (CND) Service Provider Certification and Accreditation Program," 17 December 2003
(i) NIST SP 800-137, "Information Security Continuous Monitoring for Federal Information Systems and Organizations," September 2011
(j) NGA Directive (NGAD) 8000, "Information Management and the Chief Information Officer," 09 August 2013
(k) Cyber Security Operations Cell Concept of Operations (CONOPS), 22 May 2014
(l) Administrative Update on responsibilities of the Chief Information Security Officer (CISO), from NGA IG note, 20 May 2015, (Change 1)
(m) Email from D/NGA to CoS, "Policy Signature Designation Note," 5 June 2015, (Change 2)
(n) Administrative Update on responsibilities of the Director, NGA Operations Center (NOC) and NGA Continuity Coordinator, (Change 3)

ENCLOSURE 2

RESPONSIBILITIES

1. Director, NGA (D/NGA).

a. Oversees cyber defense operations to ensure integration with the NGA mission and posture NGA in defense of current and future threats.

b. Executes and supports risk management decisions to resource, plan, and prepare for survival, continuity, recovery, and restoration of NGA's mission-critical and mission-essential ISs, applications, and data when affected by cybersecurity threats and incidents.

2. Chief Information Officer (CIO)-~~&~~-Director, IT Services (~~T~~/CIO-D/T).

a. Oversees overall coordination of enterprise cyber defense management IAW Reference (j).

b. Coordinates policies to support CSOC operations.

c. Assists Key Component (KC) Directors with guidance and direction regarding resources of high value and relevance to cyber defense expertise.

d. Establishes, implements, maintains, monitors, and reports status on ISs and networks.

e. Implements and enforces requirements to support NGA CSOC threat analysis and remediation.

f. In conjunction with the Chief Information Security Officer (CISO) and the NGA Continuity Coordinator, executes risk management and funding decisions to resource, plan, and prepare for the survival, continuity, recovery. CISO also ensures that an adequate and effective information assurance program is developed, implemented, and maintained on behalf of the CIO under the Federal Information Management Security Act. Remediation of mission-critical and mission-essential information system assets and data when affected by a cyber-security threat or incident are managed on behalf of the CISO through the CSOC.

g. Reports directly to the D/NGA on matters relating to the security of NGA networks and ISs.

h. Supports NGA's mission-essential functions.

i. Ensures a defense-in-breadth and defense-in-depth strategy is provided for the survival, continuity, recovery, and restoration of NGA ISs, applications, and data when faced with cyber threats or incidents.

j. Provides and maintains situational awareness of cyber threats directly impacting NGA's mission to ensure the confidentiality, integrity, and availability of NGA information and ISs.

k. Leads the development of the CSOC.

l. Identifies best business practices and incident monitoring and handling workflow.

3. Director, CSOC.

a. Serves as the NGA focal point for collection and reporting of cyber defense operations, and ensures appropriate escalation of significant cybersecurity events, incidents, or threats.

b. Protects NGA networks and separately operated ISs by employing programs and processes supporting information network operations and cyberspace defense operations.

c. Establishes data collection requirements to monitor, analyze, and examine cyber threats and attacks IAW Reference (k).

d. Establishes and enforces the use of tools, methodology, and best practices for cybersecurity defense to respond and remediate threats and disruptions for NGA systems and networks.

e. Oversees NGA's cybersecurity incident detection, analysis, examination, mitigation, counterintelligence review, cyber intelligence collection, and reporting (internal and external).

f. Coordinates with external agencies, combatant commands, and services on cyber defense operations, as required.

g. Integrates direct operational and support personnel from ~~T~~/CIO-*T*, Analysis Directorate (A), Security and Installations Directorate (SI), and Source Directorate (S).

4. Director, NOC.

a. Coordinate internal and external cybersecurity incident reporting requirements with CSOC to ensure reporting timelines are met using the appropriate formats and methods.

b. Provide exercise support across the NOC Enterprise to integrate response and reporting requirements to D/NGA, NGA partners, and the IC.

5. KC Directors and Career Service Heads.

a. Provide assistance (e.g., people, processes, and technology), as necessary, to support CSOC operations.

b. In conjunction with the CSOC, identify a security plan for incident monitoring and remediation for each NGA system under ~~T~~/CIO-*T* purview and ensure understanding and capabilities are provided to execute and maintain the plan.

c. Provide sufficient human capital investments to meet training requirements of the Cyber Team Liaison roles supporting NGA cyber defense and cyber operations.

d. Adequately fund and prioritize training and development requirements to certify the Cyber Team Liaison achieves and sustains relevant cyber expertise IAW Reference (h), as applicable.

GLOSSARY

DEFINITIONS

Access	Ability and means to communicate with or otherwise interact with a system, to use system resources to handle information, to gain knowledge of the information the system contains, or to control system components and functions. (Reference (c))
Chief Information Security Officer	Official responsible for carrying out the Chief Information Officer (CIO) responsibilities under the Federal Information Security Management Act (FISMA) and serving as the CIO's primary liaison to the agency's authorizing officials, information system owners, and information systems security officers. (Reference (c))
Confidentiality	The requirement that information is not disclosed to system entities (users, processes, devices) unless they have been authorized to access the information. (Reference (c))
Cyber Attack	An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information. (Reference (c))
Cybersecurity	The ability to protect or defend the use of cyberspace from cyber-attacks. (Reference (c))
Cyberspace	The interdependent network of information technology infrastructures that includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries. (Reference (c))
Defense-in-Breadth	A planned, systematic set of multi-disciplinary activities that seek to identify, manage, and reduce risk of exploitable vulnerabilities at every stage of the system, network, or sub-component lifecycle (system, network, or product design and development; manufacturing; packaging; assembly; system integration; distribution; operations; maintenance; and retirement). (Reference (c))

Defense-in-Depth	Information security strategy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and missions of the organization. (Reference (c)).
Disruption	An unplanned event that causes the general system or major application to be inoperable for an unacceptable length of time. (Reference (c))
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. (Reference (c))
Information	Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual. (Reference (c))
Information System	A discrete set of information resources organized for the collection, processing, patience, use, sharing, dissemination, or disposition of information. (Reference (c))
Integrity	The property whereby an entity has not been modified in an unauthorized manner. (Reference (c))
Risk	A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (1) the adverse impacts that would arise if the circumstance or event occurs; and (2) the likelihood of occurrence. [Note: Information system-related security risks are those risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and reflect the potential adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.]. (Reference (c))
Risk Management	The process of managing risks to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the nation resulting from the operation or use of an information system, and includes: 1) the conduct of a risk assessment; 2) the implementation of a risk mitigation strategy; 3) employment of

	techniques and procedures for the continuous monitoring of the security state of the information system; and 4) documenting the overall risk management program. (Reference (c)).
Security Plan	Formal document that provides an overview of the security requirements for an information system or an information security program and describes the security controls in place or planned for meeting those requirements. (Reference (h))
Threat	Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. (Reference (c))