INFORMATION ASSURANCE DIRECTORATE

IAD MANAGEMENT DIRECTIVE NO. 20
Dated: 31 May, 2005
Revised: 16 February 2010

(U) IA OVERSIGHT AND COMPLIANCE PROGRAM

(U) PURPOSE AND SCOPE

(U) This Management Directive prescribes policies and procedures and assigns responsibilities to ensure that activities conducted under the Director, NSA's (DIRNSA) Information Assurance (IA) authorities are conducted in a manner that safeguards the information and privacy rights of United States (U.S.) persons; complies with applicable U.S. laws, executive orders, regulations, directives, and policies; and permits fulfilling commitments to customers and partners.

(U) This Directive implements NSA/CSS Policy No. 1-23 (Reference a) by establishing an oversight and compliance (OC) program for persons engaged in activities conducted under NSA IA authorities, especially those activities that affect U.S. persons and including network defense activities. It defines the OC responsibilities of the Information Assurance Directorate (IAD) Director, IAD mission managers, other NSA/CSS organizations conducting activities under NSA's IA authorities, and the IAD Oversight and Compliance Coordinator (IA OCC).

(U) This Directive applies to all persons who, under NSA IA authorities:

- Collect, process, retain, or disseminate information to, from, or about a U.S. person, including any such information that can be retrieved by reference to a U.S. person's name or other personal identifying information;
- Have access to communications or information systems to conduct IA operations, including, but not limited to, such systems involved in penetration testing, readiness testing support, network monitoring, and communications security monitoring; or
- Access and conduct configuration or development activity on communications or information systems that support IA operations.

(U//~~FOUO~~) Signals Intelligence (SIGINT) communications collected under DIRNSA SIGINT authority to meet foreign intelligence, counter intelligence, and support to military operations requirements are governed by USSID SP0018 (Reference b) and not by this Directive.

RICHARD C. SCHAEFFER, JR.
Information Assurance
Director

DISTRIBUTION:

DJP1
DJP2 (VR)
DJP2 (Archives)

(U) This Directive supersedes IAD Management Directive 20, dated 31 May 2005.
(U) OPI: IAD Office of Oversight and Compliance (IV)
(U) No section of this document shall be released without prior approval from the IAD Office of Policy and Doctrine (I921)

TABLE OF CONTENTS

PREFACE	4
(U) POLICY	4
(U) RESPONSIBILITIES	6
(U) REFERENCES	10
(U) DEFINITIONS	10
ANNEX A (U) PROCEDURES FOR COLLECTION, PROCESSING, RETENTION, AND DISSEMINATION OF INFORMATION TO, FROM, OR ABOUT U.S. PERSONS	12
ANNEX B (U) OVERSIGHT AND COMPLIANCE TRAINING PROGRAM FOR PERSONS CONDUCTING ACTIVITIES UNDER NSA IA AUTHORITIES	15
ANNEX C (U) COMPLIANCE VERIFICATION REVIEWS	17
ANNEX D (U) HANDLING OF REPORTABLE INCIDENTS	20

PREFACE

(U) IA Mission Authorities

1. (U) Persons carrying out the DIRNSA Information Assurance (IA) activities may rely on multiple IA authorities, including the following:

a. (U) National Security Directive 42 (Reference c) designates the Director, National Security Agency (DIRNSA), as the National Manager for National Security Systems (NSS). Executive Order 12333 (Reference d) reaffirms DIRNSA's National Manager role. In accordance with NSA/CSS Policy 1-2, DIRNSA, in approving IAD's Mission and Function Statement, delegated his National Manager authority to the IAD Director. Thus, the IAD Director performs all National Manager functions.

b. (U) Executive Order 12333 authorizes intelligence agencies, including NSA, to provide specialized equipment, technical knowledge, or assistance of expert personnel for use by any U.S. Government department or agency with NSS, as well as non-NSS.[1] The Executive Order also directs that provision of assistance by expert personnel shall be approved in each case by the general counsel of the providing element or department.[2]

2. (U) All activities conducted under NSA's IA authorities must comply with the Fourth Amendment to the U.S. Constitution. The Fourth Amendment protects all U.S. persons anywhere in the world and all persons within the United States from unreasonable searches and seizures by any person or agency acting on behalf of the U.S. Government. The Supreme Court has ruled that the collection of U.S. person electronic communications may be a search and seizure within the meaning of the Fourth Amendment. Section 2.3 of Executive Order 12333 requires that collection, retention, or dissemination of information to, from, or about U.S. persons by intelligence agencies be conducted pursuant to procedures approved by the head of the Agency and the Attorney General (AG), to ensure such activities are conducted in accordance with U.S. laws, including the Fourth Amendment, executive orders, regulations, directives, and policies. To this end, Department of Defense (DoD) Directive 5240.01 (Reference e) and DoD Regulation 5240.1-R (Reference f) were approved by the AG and apply to activities conducted under NSA IA authorities. Additional specific AG-approved procedures for Communications Security (COMSEC) monitoring activities are provided in National Telecommunications and Information Systems Security Directive (NTISSD) 600 (Reference g). Together, these references provide rules to protect the information and privacy rights of U.S. persons, and this Directive implements this set of procedures.

(U) POLICY

[1] (U) FBI- Operational assistance to the FBI, and other law enforcement entities, is governed by IAD Management Directive 6, "Information Assurance Procedures Governing the Delivery of Technical Assistance to Law Enforcement," as amended 23 December 2008.

[2] (U) Please contact the office of the Associate General Counsel (Information Assurance) for applicable legal documentation.

1. (U//~~FOUO~~) All persons conducting activities under NSA IA authorities, including those who access or configure information systems that support the IA mission, shall adhere to the requirements of Reference a and this Directive. [3]

2. (U//~~FOUO~~) IAD shall implement a robust IA Oversight and Compliance (OC) program permitting the conduct of authorized IA mission functions while safeguarding the information and privacy rights of U.S. persons as afforded by Federal laws, executive orders, regulations, directives, and policies.

3. (U//~~FOUO~~) All NSA/CSS organizations conducting activities covered by this Directive shall develop and maintain local procedures detailing their compliance processes. Local procedures shall document, in detail, how each mission element complies with the provisions of this Directive, as follows:

a. (U//~~FOUO~~) Collection, processing, retention, or dissemination of information to, from, or about a U.S. person, as well as access to a communications or information system to conduct IA operations, pursuant to NSA IA authorities shall only be conducted in accordance with ANNEX A of this Directive. Local procedures used shall be documented by the organization conducting these activities. All such documented procedures must be coordinated with and approved by the IA Oversight and Compliance Coordinator (OCC) and the office of the Associate General Counsel for Information Assurance (AGC(IA)) prior to implementation. Local procedures shall be established and coordinated within thirty (30) calendar days of the establishment of new organization mission activities not covered by existing local procedures.

b. (U//~~FOUO~~) The IA OC program shall include comprehensive multi-level training (ANNEX B) for all persons conducting activities under NSA IA authorities in order to fully sensitize such personnel to their responsibilities to protect the privacy rights of U.S. persons and to other provisions of this Directive. Local procedures shall incorporate these training requirements.

c. (U) NSA/CSS organizations shall include an oversight program in accordance with ANNEX C as part of their local procedures for conducting activities under NSA IA authorities.

4. (U//~~FOUO~~) Questions and comments concerning this Directive should be submitted to the IAD Office of Oversight and Compliance (IV), NSTS 968-4277. Questions concerning the legal requirements associated with this Directive should be addressed to the Office of the AGC(IA), (D24) NSTS 966-5574.

---

[3] (U//~~FOUO~~) Examples of such activities and the organizations that conduct them under NSA IA authorities include, but are not limited to, the National Information Assurance Partnership (NIAP), Technology Directorate, Systems and Network Analysis Center (SNAC), COMSEC monitoring (i.e., Joint COMSEC Monitoring Activity (JCMA)), penetration testing and readiness testing support (Red Team and Blue Team), network monitoring (the NSA/CSS Threat Operations Center (NTOC)), Advanced Network Operations (ANO), Supervisory Control and Data Acquisition (SCADA), and their successor organizations.

(U) RESPONSIBILITIES

5. (U) The Information Assurance Director shall:

(U) Establish the position of the IA OCC to support development and maintenance of the IA OC program, consistent with Reference a of this Directive.

6. (U) IA Mission Group Chiefs, Center Chiefs, and Organization Mission Managers shall:

a. (U) Ensure that local procedures for operations within their element covered under, and consistent with, this Directive and Reference a are fully documented and have been approved by the AGC(IA) and the IA OCC prior to their implementation. Knowledge of these documented procedures shall be part of the elements' employee training.

b. (U) Ensure all organization personnel are receiving mandatory OC training in accordance with this Directive and, as outlined in ANNEX B, such training includes local procedures pertinent to the mission and function they are performing.

c. (U) Ensure that operations are compliant with all relevant oversight requirements of this Directive.

d. (U//~~FOUO~~) Direct NSA/CSS organizations operating under NSA IA authorities to craft support agreements with their customers that provide maximum flexibility and authorization to share data within NSA/CSS and DoD and, if possible, within the U.S. Government.

e. (U) Submit organization level quarterly reports to IV on "Activities Affecting U. S. Persons" and other topics requested by IV.[4]

f. (U) Ensure mission compliance officer (MCO) and mission compliance reviewer roles are designated within their mission operations in accordance with requirements of ANNEX C.

g. (U) Ensure that IV has access to organization mission personnel, oversight records, mission data, and other information as necessary for oversight purposes.

h. (U//~~FOUO~~) Unless otherwise authorized by this Directive, ensure collected data containing information to, from, or about U.S. persons is reviewed within ninety (90) calendar days from the date of its collection to determine its value and whether the data must be destroyed or can be retained for longer than ninety (90) days for IA mission purposes.

[4] (U) Cross-mission organizations outside the IAD shall provide their reports to the IG and provide IV and AGC(IA) a copy of their final reports.

i. (U//~~FOUO~~) Ensure all activities performed under IA authorities that raise questions of law or the proper interpretation of this Directive are reviewed by IV and the AGC(IA) prior to initiation.

j. (U//~~FOUO~~) Promptly report to IV and the AGC(IA) any activities operating under NSA IA authorities that may raise a question of compliance with this Directive.

k. (U//~~FOUO~~) Ensure all reportable incidents are documented and reported in a timely manner as outlined in ANNEX D of this Directive.

7. (U//~~FOUO~~) The IAD Office of Oversight and Compliance (IV) shall:

a. (U) In support of IAD:

i. ~~(FOUO)~~ Provide centralized support to the IAD Director for issues of OC associated with the IA mission;

ii. (U//~~FOUO~~) Prepare and issue consolidated quarterly reports to the NSA Inspector General (IG) regarding IAD activities affecting U.S. persons on behalf of the IAD Director. In consultation with the AGC(IA), review and comment on quarterly reports that non-IAD NSA elements may submit directly to the IG;

iii. (U//~~FOUO~~) Ensure that local procedures for NSA/CSS IA mission activities conducted under NSA IA authorities provide for timely information and situational awareness of issues of interest to the IAD Director; and

iv. (U//~~FOUO~~) Develop, implement, and maintain IA corporate level OC policies and procedures in partnership with IA OC stakeholders.

b. (U) Support NSA/CSS organizations conducting activities under NSA IA authorities by:

i. (U) Coordinating with NSA/CSS organizations and AGC(IA) to ensure that established local procedures meet the necessary standards for OC practices and procedures as required by this Directive. IV must provide documented approval of local procedures prior to their implementation.

ii. (U) Performing independent compliance reviews of local procedures, documentation, and training records within organizations operating under NSA IA authorities. These reviews do not replace the organization's internal mission compliance reviews performed in accordance with this Directive.

iii. (U) Verifying that all IA mission organization personnel are receiving core and advanced OC training pertinent to the missions and functions they perform for their organization. [5]

iv. (U) Meeting periodically with the IA mission organizations that implement mission compliance programs documented in their local procedures to provide oversight guidance and determine conformance with this Directive.

v. (U) Reviewing anomalies, issues, and questionable trends with organization mission managers, analysts, MCOs, and AGC(IA) to determine necessary corrective action or the reportability of such information to the NSA IG, AGC(IA), or external overseers.

c. (U) Oversee IA OC training program by:

i. (U) Coordinating with the AGC(IA) and organization mission managers to establish OC training requirements and develop detailed documentation and other working aids for persons subject to this Directive.

ii. (U) Ensuring that IA OC guidelines and working aids are readily available and training is provided, as necessary, for persons subject to this Directive.

iii. (U//~~FOUO~~) Partnering with ADET; SID OC; NTOC Policy, Oversight and Compliance; and AGC(IA) on specialized and new training, when required, to enhance NSA/CSS IA mission compliance with this Directive.

iv. (U) Establishing routine reviews and updates of IA OC training documentation and materials to reflect changes to the IA mission, technology utilized, or higher level policy.

v. (U) Ensuring that a notification system is in place and implemented that advises persons conducting activities under NSA IA authorities when core and advanced IA OC training is required.

vi. (U) Advising organization mission managers and group management of any apparent inconsistencies or recommended changes in their local IA OC training activities.

d. (U) Support AGC(IA) and the NSA IG by:

i. (U//~~FOUO~~) Providing support as needed to the AGC(IA) and the NSA IG in carrying out their oversight responsibilities as they relate to this Directive.

---

[5] (U) NTOC will maintain internal OC training records and provide compliance data to IV.

ii. (U) Supporting the AGC(IA) in reviewing past or ongoing activities, conducted under NSA IA authorities, for potential inconsistencies with applicable law and policy.

iii. (U) Supporting AGC(IA) in reviewing new or amended federal laws, executive orders, and DoD regulations and directives for their OC implications to the IA mission.

e. (U) Support the IAD Office of Policy by partnering with that office to develop and review necessary IA OC-related policies and directives.

f. (U) Coordinate with the OC elements of other parts of the Agency on policies and directives related to the use of NSA IA information.

g. (U) Support the NSA Director of Compliance by:

i. Assisting, as needed, to resolve corporate OC related issues involving IA activities.

ii. (U) Promptly notifying the NSA/CSS Director of Compliance about significant reportable incidents, as defined in ANNEX D.

8. (U) The Associate General Counsel for Information Assurance (AGC(IA)) shall:

a. (U//~~FOUO~~) Provide legal advice and assistance pertaining to IA OC issues, including interpretations of this Directive, to all organizations of NSA/CSS conducting activities under NSA IA authorities.

b. (U) Advise the NSA IG on its inspections and oversight of IA activities conducted under NSA IA authorities.

c. (U) Advise all persons, except for contractors, conducting activities under NSA IA authorities of new legislation and case law that may affect IA OC of IAD missions, functions, operations, activities, or practices.

d. (U) Report to the Attorney General on IA OC issues, as required, and provide copies of such reports to the DIRNSA/CHCSS and affected agency organizations.

e. (U) In coordination with IV, review and provide approval for local procedures that meet the necessary standards for OC practices and procedures, as required by this Directive.

(U) REFERENCES

9. (U) References

a. (U) NSA/CSS Policy 1-23, "Procedures Governing NSA/CSS Activities That Affect U.S. Persons," as amended, dated 11 March 2004.

b. (U) USSID SP0018, "Legal Compliance and Minimization Procedures," dated 27 July 1993.

c. (U) National Security Directive 42, "National Policy for the Security of National Security Telecommunications and Information Systems," dated 5 July 1990.

d. (U) Executive Order 12333, "United States Intelligence Activities," dated 4 December 1981, as amended 30 July 2008.

e. (U) DoD Directive 5240.01, "DoD Intelligence Activities," dated 27 August 2007.

f. (U) DoD Regulation 5240.1-R, "Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons," December 1982.

g. (U) National Telecommunications and Information Systems Security Directive (NTISSD) 600, dated 10 April 1990.

h. (U) 18 U.S.C. § 2510 et seq. (Federal Wiretap Act).

i. (U) 18 U.S.C. § 2510 note; Section 107(b) of the Electronic Communications Privacy Act of 1986, P.L. 99-508.

(U) DEFINITIONS

10. (U) The following definitions apply only to activities subject to this Directive. Terms that are defined in References f and g have the same meaning in this Directive.

a. (U) Mission Compliance Officer (MCO): An individual tasked to review the critical process steps performed by others in conducting activities under NSA IA authorities for compliance with this Directive, including, but not limited to, reviewing for proper authorizations and documentation, action plans, procedure documentation, process steps performed, system configurations, and content of reports.

b. (U) Mission Compliance Reviewer: An individual tasked to review the activities of the first line compliance officers, as needed, providing support and guidance to the

compliance officers and assessing thoroughness and consistency in overseeing mission critical process steps.

c. (U) Compliance verification: An independent review to ensure compliance with applicable laws and policies, including this Directive, of critical actions by all persons conducting activities under, or of system configurations designed pursuant to, NSA IA authorities. Compliance verification is normally conducted within the mission elements.

d. (U) Reportable incident: 1) An unauthorized collection, processing, retention, or dissemination of information that identifies a U.S. person, 2) an unauthorized access to a communications or information system to conduct NSA IA operations, or 3) events occurring during or resulting from conducting authorized IA activities resulting in consequences described in ANNEX D of this Directive. Reportable incidents include any failure to follow this Directive or applicable Federal laws, executive orders, regulations, directives, and policies that protect the information and privacy rights of U.S. persons, whether or not information was improperly acquired or released.

IAD Management Directive 20

ANNEX A
(U) Procedures for Collection, Processing, Retention, and Dissemination of Information To, From, or About U.S. Persons

1. (U//~~FOUO~~) COLLECTION AND PROCESSING

1.1. (U//~~FOUO~~) Collection and processing of information to, from, or about U.S. persons voluntarily provided by cooperating sources[6] shall be governed by Reference f as well as other applicable Federal laws, executive orders, regulations, directives, and policies and not by the rest of this section.

1.2. (U//~~FOUO~~) Consistent with Reference a, NSA/CSS activities conducted pursuant to NSA IA authorities shall be conducted in strict compliance with Federal laws, executive orders and implementing procedures, and applicable Presidential directives. Accordingly, activities conducted pursuant to NSA IA authorities shall not be initiated (or, if initiated prior to the date of this Directive and not in compliance with this Directive shall cease — except as provided for in section 1.3 — until brought into compliance) until written documentation is obtained reflecting that:

a. (U) Collection is authorized by References c and d or applicable Federal laws, executive orders, regulations, directives, and policies; and

b. (U) Collection falls within as many of the following exceptions to Reference h as is practical and applicable:

i. (U) A service provider exception exists, as evidenced by a written request made to NSA/CSS for technical assistance under the requester's service provider authority. (Note: For DoD customers, there must be documentation that the Joint Task Force – Global Network Operations, or its successor organization, made the request or is aware of the request);

ii. (U) A consent exception exists wherein the system owner certifies in writing that a program is in place to provide the following legally sufficient notification to its system users: use of such systems constitutes implied consent for monitoring for official U.S. Government purposes; or, in the determination of AGC(IA), other releasable documentation to that effect exists; or

---

[6] (U//~~FOUO~~) Information to, from, or about a U.S. person voluntarily provided by cooperating sources may include the identity of the U.S. person; including individuals and corporations, social security numbers, and other identifying information. An example of this would be the collection of information for evaluations of Commercial off-the-shelf (COTS) products or conducted through the National Information Assurance Partnership (NIAP).

iii. (U//~~FOUO~~) A COMSEC monitoring exception exists, whereby the U.S. Government department or agency requests COMSEC monitoring of its systems, in writing; provides written evidence of consent as noted in section 1.2.b(ii) above; and ensures the collection is consistent with Reference g.

c. (U//~~FOUO~~) NSA/CSS IA collection activities shall not be initiated until the IA DIR approval (or that of his designee) is granted. Such approval shall be requested in writing on a staff processing form for IA DIR's approval (or that of his designee). The staffing package shall include all written documentation required by this section and shall be vetted through AGC(IA) and IV for concurrence.

1.3. (U//~~FOUO~~) All authorized persons may access and report on NSA/CSS IA data and systems containing information potentially collected, processed, retained, or disseminated in violation of applicable law or policy, including this Directive, for the limited purpose of investigating, characterizing, or mitigating those violations. The affected mission element shall promptly notify IV and the AGC(IA) to seek appropriate additional guidance.

1.4. (U//~~FOUO~~) All selection terms used pursuant to NSA's IA authority that are likely to result in the collection of communications to, from, or about a U.S. person must: 1) be within the scope of that requested by the customer, and 2) comply with applicable law and policy, including this Directive. NSA/CSS organizations subject to this Directive shall establish and document local procedures, subject to IV and AGC(IA) approval, to ensure these requirements are met. Any selection term discovered to have resulted in the collection of information exceeding the scope of the customer's request or law or policy shall immediately upon discovery be discontinued and the information shall immediately be destroyed except: 1) as provided for in section 1.3, or 2) evidence of a crime or threat of death or serious bodily harm to any person that shall be required to be reported to the appropriate authorities. Any collection exceeding the scope of the customers request shall be considered unauthorized and subsequently documented through an incident report in accordance with annex D.

1.5. (U//~~FOUO~~) Use of selection terms is subject to oversight by IV and the AGC(IA) as follows:

a. (U//~~FOUO~~) IV shall conduct periodic independent compliance reviews of all NSA/CSS IA activities involving selection terms. These reviews shall be performed at least quarterly. These compliance reviews shall ensure that IV and AGC(IA) approved local procedures, intended to prevent use of selection terms that would exceed the scope of customer requests or violate applicable law or policy, are in place, implemented, and effective.

b. (U//~~FOUO~~) A copy of the review results will be provided to the organization mission managers and the AGC(IA). When results of the review reveal that information to, from, or about a U.S. person was collected, retained, or disseminated in a manner exceeding that authorized by the customer, or by law or policy, such information shall be reported in accordance with incident reporting procedures (ANNEX D).

2. (U) RETENTION

2.1. (U//~~FOUO~~) In accordance with Reference f, data recorded or otherwise retained under authorized activities conducted under NSA IA authorities and containing or potentially containing information to, from, or about a U.S. person, shall be evaluated within ninety (90) calendar days of collection under local procedures that have been reviewed and approved by IV and AGC(IA), to determine if there is a legitimate mission-related reason to retain the information for longer than ninety (90) days. If no legitimate reason for retention is identified under these procedures, the information shall be destroyed. The ninety (90)-day period, described above, applies unless the data owner has provided for a shorter retention period.

2.2. (U//~~FOUO~~) If the data is determined to hold legitimate value for the approved mission activity, it may be retained beyond the ninety (90) calendar day period, up to the time approved in writing by the data owner, in accordance with written documentation approved by AGC(IA). The duration of data retention will comply with records disposition schedules, approved by the National Archives and Records Administration, for the files or records in which the information is retained. However, the duration of data retention shall not exceed: (1) the period of time needed to achieve the mission, (2) the retention duration approved by the data owner, and (3) five (5) years without a review for either destruction or justifiable longer retention by the mission element in consultation with IV.

3. (U) DISSEMINATION

3.1. (U//~~FOUO~~) In accordance with Reference f, dissemination of reports containing information to, from, or about a U.S. person voluntarily provided by cooperating sources, shall be governed by this Directive and internal NSA/CSS policies (such as NSA/CSS Policy 3-13, "Information Technology Product or System Vulnerabilities" or its successor), but is not subject to the limitations in subsections 3.2 and 3.3.

3.2. (U//~~FOUO~~) Subject to the limitation in subsection 3.4, dissemination of information collected pursuant to the service provider or consent exceptions in sections 1.2(b)(i) and (ii) is governed by Reference f. A dissemination may be made to any NSA employee (including foreign integrees) or NSA contractor affiliate who is authorized to receive it, and who has a need for the information in the course of official duties. Such information also may be released to others in the DoD, intelligence, and law enforcement communities when such release is authorized and in accordance with written documentation approved by AGC(IA).

3.3. (U//~~FOUO~~) Subject to the limitation in subsection 3.4, dissemination of information collected pursuant to the COMSEC monitoring exception in section 1.2(b)(iii) is governed by Reference g.

3.4. (U) All proposed disseminations of information constituting privileged communications to, from, or about a U.S. person (e.g., attorney/client, doctor/patient), and all information concerning criminal activities or criminal or judicial proceedings in the U.S. must be reviewed by the Office of General Counsel prior to dissemination.

IAD Management Directive 20

ANNEX B
(U)Oversight and Compliance Training Program for Persons Conducting Activities under NSA IA Authorities

1. (U) APPLICABILITY

(U) This Annex applies for training purposes to all persons conducting, or who may conduct, activities under NSA IA authorities.

2. (U) POLICY

2.1. (U//~~FOUO~~) IA OC Core Training – All persons[7] conducting activities under NSA IA authorities shall receive IA OC core training at least annually to familiarize them with the basic Federal laws, executive orders, regulations, directives, and policies that govern NSA IA mission operations. Core training will be in accordance with Reference a and, at a minimum, shall include familiarization with References c and d; Reference f, Procedures 1 through 4, 10, 14, and 15; and this Directive. Testing shall be administered to verify applicable knowledge, as appropriate.

2.2. (U//~~FOUO~~) IA OC Advanced Training – All persons conducting activities under NSA IA authorities that have the potential for violations of this Directive, as determined by IV, shall have additional advanced IA OC training at least annually. Advanced training shall familiarize such persons with additional applicable legal and policy requirements to further minimize the potential for violations of this Directive. The actual advanced training required for each mission activity shall be determined and agreed upon by mission management, IV, and the AGC(IA). As new missions and or procedures emerge, training requirements shall be reviewed for adequacy and adjusted as agreed to be appropriate.

2.3. (U//~~FOUO~~) IA OC MCO Training – All NSA/CSS employees designated to perform as MCOs within mission operations shall first complete and be current (within one year) in the IA OC training required for the mission activity to which they are assigned. Those designated MCO employees must be current in special MCO training as shall be determined by a consensus of mission management, the IA OCC, and AGC(IA).[8]

2.4. (U) All training requirements and materials, including local procedures and this Directive, shall be reviewed as needed (e.g., when a significant change to mission procedure occurs) but no less than bi-annually. The reviews shall be conducted by IV, AGC(IA), and mission operations management to determine whether these materials continue to adequately

[7] For the purpose of this Annex, "Persons" includes civilians, contractors, military, military reservists, interns, assignees, and integrees.

[8] MCOs perform inherently governmental functions and, therefore, contractors shall not be assigned as MCOs.

encompass the latest mission functions, methods, and procedures used by mission operations. Any recommended changes to the training materials shall be submitted to IV and the AGC (IA) for approval prior to implementation.

3. (U) PROCEDURES

3.1. (U) The training of persons conducting activities under NSA IA authorities shall include guidance concerning the requirements and restrictions of applicable Federal laws, executive orders, regulations, directives, and policies. NSA/CSS employees conducting COMSEC monitoring activities shall be specifically trained on the requirements and restrictions of Reference g and successor directives.[9]

3.2. (U) The use of equipment for training purposes by persons conducting activities under NSA IA authorities is subject to the following limitations:

a. (U//~~FOUO~~) To the maximum extent practical, use of such equipment for training purposes shall be directed against targets that are under current authorization for mission operation.

b. (U//~~FOUO~~) Communications to, from, or about a U.S. person collected during training sessions may not be retained unless such content has been collected within the limitations of an authorized mission operation, in accordance with law and policy, including this Directive.

3.3. (U) The limitations in paragraph 3.2. do not apply in the following instances:

a. (U//~~FOUO~~) Public broadcasts or distress signals; and

b. (U) Minimal acquisition of information as required for calibration purposes.

[9] (U) Only U.S. Government employees may perform COMSEC monitoring. Section 107(b) of the Electronic Communications Privacy Act of 1986, P.L. 99-508.

IAD Management Directive 20

ANNEX C
(U) Compliance Verification Reviews

1. (U) PURPOSE

1.1. (U) It is essential that every effort be made to safeguard the information and the privacy rights of U.S. persons. It is also essential that NSA/CSS conduct its IA mission activities using procedures that comply with applicable Federal laws, executive orders, regulations, directives, and policies, including this Directive. Compliance may be verified using a combination of automated mechanisms that prevent or minimize policy violations as well as conducting mission compliance reviews under local procedures to detect any compliance violations that may occur or have occurred. Establishing automated methods to prevent policy violations is preferred to post-operation compliance reviews. However, organizations subject to this Directive shall establish a comprehensive set of automated and manual procedures to ensure policy violations are prevented and detected. Additionally, organizations subject to this Directive shall implement a rigorous compliance verification regime to ensure those insurance procedures are in place, implemented, and effective.

1.2. (U) Compliance verification will be included as an integral part of the documented local procedures for any NSA/CSS mission operation conducted under NSA IA authorities. As part of the organization's mission procedures, compliance verification will provide a process to review accuracy of critical process steps and reduce inadvertent mishandling of information to, from, or about a U.S. person. Assigned mission compliance reviewers shall provide the added benefit of mission expertise to ensure consistency in procedures across multiple mission projects and assist the analysts and primary MCOs in resolving issues relative to functions such as sensor programming or monitoring activity decisions.

1.3. (U) Within the IAD, the IV office will perform process compliance reviews and will address the end-to-end processes of mission activities to ensure proper correlation between procedural documentation, actual procedures performed, and NSA IA authorities. Within cross-mission NSA organizations operating under NSA IA authorities, process compliance reviews shall be performed by IV, unless the cross-mission organization can provide alternate methods of compliance review such as may be performed by their indigenous OC personnel and, on which it has attained IV concurrence.

2. (U) PROCEDURES

2.1. (U) Prior to the initiation of any mission activity that is subject to this Directive and conducted under NSA IA authorities on behalf of any client external to NSA/CSS , a manager responsible for the mission element conducting the activity shall verify and document that the mission element:

a. (U) Has been delegated the authority to conduct the mission and the source of that authority (e.g., E.O. 12333, NSD-42);

b. (U) Has been provided authorization from the appropriate Office of Primary Interest (the "data owner") to access data necessary to conduct the mission;

c. (U) Has a written statement from the data owner concerning the purposes for which the data may be used and, with whom the data may be shared; and

d. (U) Has a written statement from the data owner that appropriate "notice and consent" procedures are in place.

2.2. (U) The mission manager shall locally maintain records that are related to the requirements set forth in section 2.1. above, and provide copies to IV.

2.3. (U) Compliance with applicable laws and policies, including this Directive, shall be enforced through a combination of system design features, system configuration settings, and manual verification procedures. Taken together, these measures shall either preclude the possibility of violations, or deter them by providing effective detection capabilities.

a. (U) Compliance verification records shall be protected from unauthorized modification during their generation, storage, and retrieval.

b. (U) Actions subject to compliance review shall be described in mission element local procedures. At a minimum, actions or decisions reviewed shall include those with the potential to:

i) Cause the unauthorized collection, retention, or dissemination of information to, from, or about a U.S. person;

ii) Operate outside the boundary of approved procedures pursuant to this Directive; or

iii) Otherwise violate this Directive. Compliance verification actions include, but are not limited to, the programming of selectors, filters, sensing devices, or other query systems; the creation and dissemination of reports created from collected data containing such information; and population of routing tables or other automated systems that control or direct information subject to this Directive.

c. (U) No compliance verification activity (as described above) shall be initiated until an MCO from within the mission organization has been assigned to that activity. Assigned MCO shall be senior to (by either position or grade) or be organizationally independent of those performing the actions being monitored and must be current on required oversight training.

d. (U) Each MCO shall be assigned a mission compliance reviewer from within his/her corresponding mission organization. Mission compliance reviewers shall perform quality

control checks sufficient to provide assurance that MCOs are correctly performing their intended functions. All mission compliance reviewers shall be senior (by position or grade) to the MCOs they review.

2.4. (U) Within the IAD, IV will coordinate with mission operations to develop and schedule end-to-end procedure compliance reviews. Reviews may cover any individual portion of or the entire activity process and documentation, and may periodically include review of compliance verification procedures and data. Within cross-mission NSA organizations operating under IA authorities, IV will coordinate procedure compliance reviews, process reviews, or other assurance methods with appropriate authorities within the cross mission organizations.

IAD Management Directive 20

ANNEX D
(U) Handling of Reportable Incidents

1. (U) SCOPE

(U//~~FOUO~~) This annex addresses the handling and documentation of reportable incidents that occur during activities conducted by NSA/CSS mission organizations under IA authorities. This annex also provides local mission operations procedures for rapid leadership notification of events of significant interest that may occur during mission operations.

2. (U) PURPOSE

(U//~~FOUO~~) It is essential that all reportable incidents are documented with concise information and appropriately reported, in a timely fashion, to all parties having a stakeholder interest in the incident. All reportable incidents shall be recorded and reported, whether they were the result of intentional actions, human error, or automated system breakdown or malfunction.

(U//~~FOUO~~) A reportable incident shall include any situation in which IA authorities were improper or improperly applied, or IA approved procedures were violated, whether or not the violation actually resulted in the collection, retention, dissemination or reporting of U.S. person information.

3. (U) PROCEDURES

3.1. (U) Reporting General Incidents

3.1.1. (U//~~FOUO~~) Incidents involving the violation of IA Operational Authorities or Approved Procedures for the IA mission shall be recorded and reported within one (1) business day (24 hours – weekends and holidays excluded) of recognition of the event to the following recipients:

a. (U) Immediate Mission Management;

b. (U) IAD Oversight and Compliance (IV)[10]; and

c. (U) AGC(IA).

[10] (U//~~FOUO~~) NTOC shall report incidents to the NTOC Policy, Oversight and Compliance Office (V07), which shall distribute reports as appropriate.

3.1.2. Reportable Incidents include, but are not limited to, the following:

a. (U//~~FOUO~~) Any unauthorized collection, retention, or dissemination of U.S. person information;

b. (U//~~FOUO~~) Any provision of COMSEC monitoring or readiness testing support to a U.S. Government organization outside the bounds of an approved written support agreement;

c. (U//~~FOUO~~) Any provision of COMSEC monitoring or readiness testing support to a U.S. government organization without all required authorization and agreement documentation in place;

d. (U//~~FOUO~~) Any handling or retention of data collected under IA authorities in such a manner as to permit unauthorized access to that data;

e. (U//~~FOUO~~) Failure to follow a provision of local policy or procedure;

f. (U//~~FOUO~~) Unauthorized use of a real U.S. person name or other identifying information

(b)(3)-P.L. 86-36

g. (U//~~FOUO~~) Use of sexually suggestive or pornographic material as part of an IA operation;

h. (U//~~FOUO~~) Use of material that is insensitive based on racial, cultural, gender, sexual orientation, disability or religious criteria, age, national origin, or genetics as part of an IA operation;

3.2. Reporting of Items of Significant Interest to Senior Leadership

3.2.1. Even if all IA activities are carried out in accordance with IA authorities and approved procedures, the occurrence of unexpected events that warrant documentation and timely reporting through the chain of command could occur. For example, if an event does not involve a violation of authorities or procedures, but resulted from an activity performed under IA authorities, an incident report shall still be generated. Thus, incident reporting permits trend analysis and helps identify the need for review of policy or procedures for potential improvement.

3.2.2. It is essential that the local mission management understand the types of events that warrant immediate notification to senior leadership. The following list is not all inclusive, but suggests the types of issues that should be considered for priority reporting:

a. (U//~~FOUO~~) Physical damage to U.S. Government or private property;

b. (U//~~FOUO~~) Extensive and irreplaceable destruction of U.S. Government information (e.g., destruction of on-line databases that are not otherwise backed-up);

c. (U//~~FOUO~~) Damage to mission infrastructure or components that will disable or significantly degrade client mission operations;

d. (U//~~FOUO~~) Compromise of classified material;

e. (U//~~FOUO~~) Events that may trigger media attention or cause significant embarrassment to the Agency or IC community;

f. (U//~~FOUO~~) Denial of service of mission critical services for large segments of U.S. or foreign users (e.g., shut-down of network services for a major command, or a commercial provider);

g. (U//~~FOUO~~) Events compromising national intelligence networks or national intelligence communications;

h. (U//~~FOUO~~) Loss of control or public exposure of personal privileged information (e.g., social security numbers, home addresses, phone numbers, medical or psychological information, financial information, private correspondence or data) of U.S. persons;[11] or

i. (U//~~FOUO~~) Initiation of criminal investigations by U.S. or foreign law enforcement agencies (possibly due to the breakdown of Trusted Agent networks).

3.2.3. (U//~~FOUO~~) Local mission procedures shall include how to report these events through management in an expedient manner and, as appropriate, include notification to the following:

a. (U//~~FOUO~~) IA Director, IA Deputy Director, or IAD Chief of Staff (reporting after normal operating hours would be through the Senior Information Assurance Officer (SIAO) on duty in the NSOC);

b. (U) AGC(IA); and

c. (U) IAD Oversight and Compliance (IV).

[11](U) NSA/CSS Policy 1-22 defines "personal information" as: "Information about an individual that is intimate or private to the individual, as distinguished from information related solely to the individual's official functions or public life."

3.3. (U//~~FOUO~~) Group, center, and subordinate levels of management may impose additional reporting requirements beyond those stated in this annex, as long as they do not interfere with meeting the reporting thresholds and timelines described above.

3.4. (U//~~FOUO~~) For all reported incidents, an initial review and analysis will be made by IV,[12] with guidance from AGC(IA), as needed. Review of the incidents shall permit a determination of the completeness of the report, and permit requests for any needed clarifying information about the incident. IV, in consultation with the AGC(IA), will make a determination of what, if any, immediate action must be taken. IV will ensure the incident is properly reported to the NSA Inspector General (IG), including any end-of-quarter IG report.

[12] (U) V07 would perform initial review and analysis for NTOC based IA related incidents.

NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE
NSA/CSS POLICY 1-58

Issue Date: 24 March 2011
Revised:

(U) CYBERSPACE OPERATIONS AND EQUITIES ADJUDICATION

(U) PURPOSE AND SCOPE

(U//~~FOUO~~) This policy governs the Signals Intelligence and Information Assurance missions of NSA/CSS in conducting and supporting integrated U.S. Government [redacted] *cyberspace operations* (References a, b, c, d, e and f) and in adjudicating mission equities.

(U//~~FOUO~~) It provides direction for NSA/CSS element support to U.S. Cyber Command to achieve *integrated cyberspace operations* as envisioned in Secretary of Defense Memorandum, "Establishment of a Subordinate Unified U.S. Cyber Command Under U.S. Strategic Command for Military Cyberspace Operations" (Reference c), and implements portions of National Security Presidential Directive-54/Homeland Security Presidential Directive-23, "Cybersecurity Policy" (Reference d) and related subordinate plans, including the "Deployment of Automated Defense Sensors Across Executive Branch Federal Systems Implementation Plan" (Reference e).

(U) This policy applies to all NSA/CSS elements worldwide.

KEITH B. ALEXANDER
General, U.S. Army
Director, NSA/Chief, CSS

Endorsed by
Associate Director for Policy

Encls:
(U) Annex A – Equities Adjudication

Policy 1-58 Dated: 24 March 2011

(U) Annex B – Cryptanalytic Services

DISTRIBUTION:
DJP1
DJP6 (VR)
DJP6 (Archives)

(U) This Policy supersedes Policy 1-58 dated 24 November 2009.
(U) OPI: Corporate Policy, DJP1, 963-3086s.
(U) No section of this document, regardless of classification, shall be released without approval from the Office of Policy and Records (DJP).

(U) POLICY

1. (U//~~FOUO~~) NSA/CSS shall [redacted] enable and enhance U.S. Government [redacted] cyberspace operations (References a, b, c, d, e and f) and relevant equities are addressed.

2. (U//~~FOUO~~) NSA/CSS elements shall, to the maximum extent permissible by law and policy and consistent with NSA/CSS authorities, actively collaborate with elements of the U. S. Government, including the Department of Defense (DoD), the Intelligence Community (IC), and other U.S. Government departments or agencies [redacted]

3. (U//~~FOUO~~) As part of Office of the Director of National Intelligence (ODNI)-mandated information sharing efforts and to support the Department of Homeland Security (DHS) mission to protect *Federal systems*, NSA/CSS elements shall provide *threat* or *vulnerability* information to U.S. government [redacted] at the lowest classification level possible to facilitate its use in cyberspace operations [redacted]

4. (U//~~FOUO~~) To facilitate the holistic integration of cyberspace operations, when the [redacted]

5. (U//~~FOUO~~) In recognition of the threat posed by foreign adversaries to the nation's information systems and critical infrastructure, NSA/CSS elements shall provide information about threats or vulnerabilities [redacted]

[redacted] Information shall be provided in accordance with established procedures and with appropriate notification to stakeholders (References f, o, t, u, v, w and x).

6. (U//~~FOUO~~) [redacted]

7. (U) This policy shall be implemented in compliance with public law, policies and other applicable guidance, including those that protect the information rights and privacy of U.S. persons (References y, z, aa and ab).

(U) RESPONSIBILITIES

(b)(3)-P.L. 86-36

8. (U//~~FOUO~~) Recognizing that the greatest concentration of technical expertise and operational capability for conducting cyberspace operations resides in the USCS, NSA/CSS elements shall, in accordance with their respective authorities and mission:

a. (U//~~FOUO~~) Leverage the capabilities of the USCS to provide an integrated response to cyber threats and opportunities when conducting or providing assistance to authorized U.S. Government [redacted] cyberspace operations (References a, b, c, d, e, and f);

b. (~~C~~// [redacted]) Provide representation to an NSA/CSS Equities Adjudication Board and Senior Review Board, as appropriate. (See Annex A for details.)

[redacted] Existing equities policies or deconfliction processes (to include those in References r and s) shall be reviewed to ensure compliance with this policy. When an equity is identified for which no adjudication process exists or when parties to an existing equities process are unable to reach consensus on the outcome of an equities decision, the equity shall be adjudicated in accordance with Annex A.

c. (U//~~FOUO~~) In response to validated U.S. government requirements, develop and provide [redacted] to achieve U.S. objectives in cyberspace, including national objectives set forth in the "*Comprehensive National Cybersecurity Initiative*" and related subordinate plans [redacted] These include the following specific initiatives:

1) (U//~~FOUO~~) Participate in U.S. Government *cybersecurity* initiatives to assist DHS [redacted] (b)(3)-P.L. 86-36

2) (U//~~FOUO~~) Enhance the security of U.S. Government *National Security Systems*;

3) (U//~~FOUO~~) [redacted]

4) (U//~~FOUO~~) Expand cyber education and training capabilities;

d. (U//~~FOUO~~) Disseminate threat, vulnerability, mitigation and warning information [redacted] to include the following:

1) (U) Indications and warning of threats to the United States; and,

(b)(3)-P.L. 86-36

2) (U) Threat information from any source, including threats to U.S. critical infrastructure;

e. (U//~~FOUO~~) [redacted]

f. (U//~~FOUO~~) In response to validated DoD requirements, [redacted] enable rapid and sustained improvement in the speed, agility and effectiveness of *DoD cyberspace operations* (References c, g, and ac). These include the following requirements:

1) (U//~~FOUO~~) [redacted]

2) (U//~~FOUO~~) [redacted] (b)(3)-P.L. 86-36

3) (U//~~FOUO~~) [redacted]

4) (U//~~FOUO~~) [redacted]

5) (U//~~FOUO~~) Facilitate the training and oversight of, and mission collaboration with, USCYBERCOM personnel.

g. (U//~~FOUO~~) In response to validated DHS requirements, develop and provide [redacted]

h. (U//~~FOUO~~) In accordance with DHS authorities and mission, coordinate with DHS when providing *technical assistance* to:

1) (U//~~FOUO~~) [redacted]

2) (U//~~FOUO~~) [redacted]

(b)(3)-P.L. 86-36 i. (U//~~FOUO~~) [redacted]

[redacted]

(b)(3)-P.L. 86-36

j. (U//~~FOUO~~) In recognition of the importance of a comprehensive approach to cybersecurity, as permissible by law and policy, work with the ODNI, DoD, DHS, and other governmental and non-governmental entities to facilitate partnerships to systematically address cyber-related threats that span both government and industry (References d, t, u, v, x, and af);

(b)(1)
(b)(3)-P.L. 86-36

k. (U//~~FOUO~~) To ensure the security of NSA/CSS information systems, NSA/CSS elements shall notify the Office of Counterintelligence (Q3) of any indication of foreign cyber operations targeting or successfully exploiting or compromising any NSA/CSS information network or system (Reference ag);

l. ~~(C//~~ [redacted]

m. ~~(S//~~ [redacted]

n. ~~(S//~~ [redacted] Ensure cyber indicators of known or suspected malicious activity [redacted] are submitted upon identification and when operationally feasible[1] for equities adjudication or deconfliction to expedite, whenever possible, their use in cyberspace operations, to include network defense or inclusion in automated defense sensors (References d, e, f, ae, ah and ai);

o. (U//~~FOUO~~) With other NSA/CSS elements, develop automated mechanisms to facilitate equities adjudication and operational deconfliction of threat and vulnerability information;

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36

[1] ~~(S//~~ [redacted]

[redacted]

(b)(1)
(b)(3)-P.L. 86-36

p. (U//~~FOUO~~) Review and develop new or update existing policies, procedures, technical solutions and operational constructs [redacted]

(b)(3)-P.L. 86-36

q. (U//~~FOUO~~) Identify and address impediments to the effective implementation of this policy. As required, NSA/CSS elements shall work with OGC and relevant oversight and compliance bodies when existing authorities or procedures may impede effective implementation [2]; and work with DJ to modify existing policies and procedures, and propose and seek approval for new policies and procedures as needed to achieve the objectives stated herein.

9. (U) The Director, Signals Intelligence Directorate (SID), shall:

a. ~~(C//~~ [redacted]

b. ~~(S//~~ [redacted]

(b)(1)
(b)(3)-50 USC 403
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

c. ~~(S//~~ [redacted] To increase understanding of adversarial threats, capabilities and intentions; [redacted]

d. ~~(S//~~ [redacted] Conduct SIGINT targeting and operations to [redacted]

[2] (U~~FOUO~~) This may include seeking additional authorities or approval of new procedures from the Secretary of Defense, the U.S. Attorney General or the Director of National Intelligence.

(b)(1)
(b)(3)-P.L. 86-36

e. (~~S//~~) Support the Director, NSA (DIRNSA) in his role as the Executive Secretary responsible for deconfliction of U.S. government CNE and CNA activities (References p and q);

f. (~~S//~~) Under the guidance of the Secretary of Defense, the Attorney General and the DNI, coordinate requests for and support authorized CNA planning and execution with USCYBERCOM, Combatant Commands and other DoD elements, (References c, g, and ac);

(b)(1)
(b)(3)-P.L. 86-36

g. (~~S//~~) Support authorized CNA activities

h. (~~S//~~) Support authorized CNA technology development and targeting efforts (References c, g, and ac);

)(1)
)(3)-P.L. 86-36

i. (~~S//~~)

j. (~~C//~~) Develop and deploy cryptanalytic capabilities to

k. (U//~~FOUO~~) Provide, upon request, SIGINT technical assistance to U.S. Government departments and agencies (Reference a);

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36

l. (U//~~FOUO~~) Provide cryptanalytic services to U.S. Government departments or agencies and other authorized recipients as part of U.S. national cybersecurity initiatives in accordance with Annex B, "Cryptanalytic Services," of this policy (References d and e);

m. (~~S//~~) Provide SIGINT support in response to foreign intelligence requirements,

n. (~~S//~~)

o. (~~C//~~)

b)(1)
b)(3)-P.L. 86-36

[redacted]

10. (U) The Director, Information Assurance Directorate (IAD), shall:

a. ~~(C/~~ [redacted]

b. ~~(S/~~ [redacted]

c. ~~(S/~~ [redacted]

d. (U//~~FOUO~~) In consultation with the Secretary of Defense and the ODNI, work to enhance the security of U.S. Government National Security Systems against cyber intrusion and attack by implementing specific defensive measures to significantly reduce malicious activity and enhance the protection of these networks from the full range of cyber threats (References b and d);

e. (U//~~FOUO~~) Develop architectures and capabilities to identify and reduce vulnerabilities of U.S. Government National Security Systems and increase the security of National Security System networks (References b and d);

f. ~~(S/~~ [redacted] Conduct predictive and trend analyses to better understand and anticipate cyber threat and technology developments (Reference d);

g. (U//~~FOUO~~) Strengthen enterprise-wide cross-domain capabilities and use strong identity protection to enable greater information sharing among key U.S. Government cyber organizations (Reference d);

h. ~~(S/~~ [redacted]

i. (U//~~FOUO~~) Conduct operations to identify and characterize adversarial penetrations of U.S. government National Security System networks (References b, d and ag);

j. (U//~~FOUO~~) Provide, upon request, IA technical assistance to U.S. Government departments and agencies (Reference a);

k. (U//~~FOUO~~) Provide IA technical assistance to owners or operators of U.S. Government National Security Systems (References a and b);

l. (U//~~FOUO~~) Provide IA technical assistance to owners or operators of non-National Security Systems and, where such assistance is not authorized by Reference a, provide it consistent with the Federal Information Security Management Act and procedures agreed to by NSA/CSS and the National Institute of Standards and Technology (References a and ae);

(b)(3)-P.L. 86-36

m. (U//~~FOUO~~) [redacted]

n. (U//~~FOUO~~) [redacted]

o. (~~C//~~ [redacted]

p. (U//~~FOUO~~) As the National Manager for IA education and training relating to U.S. Government National Security Systems, partner with the Associate Director for Education and Training, DoD, DHS and other U.S. Government organizations to expand cyber education and training capabilities (References b and d).

11. (U) The Director, NSA/CSS Threat Operations Center (NTOC), employing authorities delegated by Directors of SID and IAD, shall:

(b)(1)
(b)(3)-P.L. 86-36

a. (U//~~FOUO~~) Serve as a driver for integrated cyberspace operations, providing a venue for the planning, coordination and synchronization of authorized DoD and U.S. government cyberspace operations (References c and d);

(b)(1)
(b)(3)-P.L. 86-36

b. ~~(S//~~ [redacted] In cooperation with DoD and U.S. Government departments and agencies, build and maintain a common cyber operating picture that provides an understanding of the global cyber environment and supports multiple missions, including CNE, CND and support to Network Operations and CNA (References a, b, c and d);

c. ~~(S//~~ [redacted] Serve as a leader for intrusion-detection analysis and response actions, providing direct support, as authorized, to DoD and other U.S. Government departments and agencies at the national level (References a, b, c and d);

d. (U//~~FOUO~~) Serve as a national cybersecurity center, in accordance with Reference d;

(b)(1)
(b)(3)-P.L. 86-36

e. (U//~~FOUO~~) Provide indications and warnings of threats to U.S. networks or information systems (References b, d and al);

f. ~~(S//~~ [redacted]

g. ~~(S//~~ [redacted]

h. ~~(S//~~ [redacted]

i. (U//~~FOUO~~) [redacted]

(b)(3)-P.L. 86-36

j. ~~(C//~~ [redacted]

k. ~~(C//~~ [redacted]

l. (C/[redacted]

m. (U//~~FOUO~~) [redacted]

12. (U) The Director, Technology Directorate, shall:

a. (U//~~FOUO~~) Ensure that mission modernization architectures facilitate unity of effort [redacted] (b)(3)-P.L. 86-36

b. (U//~~FOUO~~) In coordination with NTOC, and as authorized, maintain automated defense architectures in support of USCYBERCOM and other NSA/CSS partners and customers (References d, e, ah and ai);

c. (U//~~FOUO~~) In accordance with ODNI- and DoD-promulgated standards, provide certification and accreditation of automated defense systems on NSANet and other DoD networks, as required, in support of USCYBERCOM and other NSA/CSS National Security System partners and customers (References d, e, g, am and an); and,

d. (S/[redacted]) Provide technical assistance and security certification assistance to DHS in support of DHS cybersecurity efforts using automated defense technologies (References d, e, am and an).

13. (U) The Director, National Security Operations Center (NSOC), shall:

a. (S/[redacted]) Maintain CRITIC criteria for cyber events and execute CRITIC reporting upon indication of:

1) (S/[redacted]) [redacted] (b)(1) (b)(3)-P.L. 86-36

2) (S/[redacted]) [redacted]

b. (U//~~FOUO~~) [redacted]

(b)(1) (b)(3)-50 USC 403 (b)(3)-P.L. 86-36

)(1)
)(3)-P.L. 86-36

14. ~~(C//~~ [redacted]

15. ~~(S//~~ [redacted]

16. (U//~~FOUO~~) The Associate Directorate for Education and Training shall partner with NSA/CSS mission elements, DoD, DHS and other U.S. Government organizations to expand cyber education and training capabilities (Reference d).

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36

(U) REFERENCES

17. (U) References:

a. (U) Executive Order 12333, as amended, *"United States Intelligence Activities,"* dated July 2008.

b. (U) NSD-42, *"National Policy for the Security of National Security Telecommunications and Information Systems,"* dated 5 July 1990.

c. (U) Secretary of Defense Memorandum, *"Establishment of a Subordinate Unified U.S. Cyber Command Under U.S. Strategic Command for Military Cyberspace Operations,"* dated 23 June 2009.

d. (U) NSPD-54/HSPD-23, *"Cybersecurity Policy,"* dated 8 January 2008.

e. (U) *"Deployment of Automated Defense Sensors Across Executive Branch Federal Systems Implementation Plan,"* dated 22 September 2008.

(b)(3)-P.L. 86-36

[redacted]

g. (U) CDRUSSTRATCOM CONPLAN 8039, *"Cyberspace Operations,"* dated 3 June 2008.

h. (U) Intelligence Community Directive 501, *"Discovery and Dissemination or Retrieval of Information Within the Intelligence Community,"* dated 21 January 2009.

(b)(3)-P.L. 86-36

i. (U) NSA/CSS Policy 1-9, *"Information Sharing,"* dated 26 May 2005.

[redacted]

(b)(1)
(b)(3)-P.L. 86-36

[redacted] (b)(3)-P.L. 86-36

m. (U//~~FOUO~~) NSCID 6, *"Signals Intelligence,"* dated 17 February 1972.

[redacted] (b)(3)-P.L. 86-36

(b)(1) OGA

o. (U) HSPD-7, *"Critical Infrastructure Identification, Prioritization and Protection,"* dated 17 December 2003.

NSC

p [redacted]

q. (U//~~FOUO~~) *"Trilateral MOA Among DoD, DoJ and the IC Regarding CNA and CNE Activities,"* dated May 2007.

r. (U//~~FOUO~~) NSA/CSS Policy 3-13, *"Information Technology Product or System Vulnerabilities,"* dated 1 July 2005.

s. (U) ISS-155-06, *"Policy and Guidance for Reporting and Dissemination of SIGINT Technical Information,"* dated 12 October 2007.

t. (U) *"Homeland Security Act of 2002,"* 6 USC 101(9), dated 19 November 2002.

u. (U) *"Critical Infrastructures Protection Act of 2001,"* Section 1016(e) of Public Law 107-56, USA PATRIOT Act, (42 U.S.C. 5195c(e), dated 26 October 2001.

v. (U) Executive Order 13388, *"Further Strengthening the Sharing of Terrorism Information to Protect Americans,"* dated 25 October 2005.

w. (U) DCID 7/4, *"Critical Information,"* dated 2 January 2001.

x. (U) Public Law 108-456, *"Intelligence Reform and Terrorism Protection Act of 2004,"* dated 17 December 2004.

y. (U) DoD Regulation 5240.1-R, *"Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons,"* dated 7 December 1982.

z. (U) *"Foreign Intelligence Surveillance Act of 1978,"* as amended (2008).

aa. (U) NSA/CSS Policy 1-23, *"Procedures Governing NSA/CSS Activities that Affect U.S. Persons,"* 27 December 2007.

ab. (U/~~FOUO~~) USSID SP0018 – *"Legal Compliance and Minimization Procedures,"* dated 27 July 1993.

ac. (U) *"National Military Strategy for Cyberspace Operations,"* dated December 2006.

ad. (U) *"White House Cyberspace Policy Review,"* dated 29 May 2009.

ae. (U) *"Federal Information Security Management Act of 2002,"* dated 17 December 2002.

af. (U) DoDD 3020.40, *"Defense Critical Infrastructure Program,"* dated 19 August 2005.

ag. (U) NSA/CSS Policy 5-31, *"NSA/CSS Counterintelligence Program,"* dated 27 January 2005.

ah. (U) DoDD O-8530.1, *"Computer Network Defense,"* dated 8 January 2001.

ai. (U) DoDI O-8530.2, *"Support to Computer Network Defense,"* dated 9 March 2001.

aj. (U) NSPD-26, *"Intelligence Priorities,"* dated 24 February 2003.

ak. (U) Department of Homeland Security, *"National Infrastructure Protection Plan,"* dated January 2009.

al. (U) CJCSM 6510.01, *"Information Assurance and Computer Network Defense,"* dated 18 March 2005.

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

an. (U) DoD Directive 8500.01E, *"Information Assurance,"* dated 24 October 2002.

ao. (U) USSID CR1305, *"Cryptologic Information Report,"* dated 23 July 2008.

(U) DEFINITIONS

18. (U) Civil Authorities – Nonmilitary Federal, State, or local government agencies (Source: DoDD 3025.15).

19. (U) Comprehensive National Cybersecurity Initiative – As used in this policy, refers to an integrated and holistic national approach to cybersecurity practices to achieve the goals outlined in NSPD-54/HSPD-23, "Cybersecurity Policy" (Reference d). Core to this strategy is the "bridging" of historically separate cyber defensive missions with law enforcement, intelligence, counterintelligence, and military capabilities to address the full spectrum of cyber threats from remote network intrusions and insider operations to supply chain vulnerabilities (Reference ad).

20. (U) Computer Network Attack (CNA) – Operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves (Source: DoDD 3600.01). (b)(1) (b)(3)-18 USC 798 (b)(3)-50 USC 403 (b)(3)-P.L. 86-36

21. (U) Computer Network Defense (CND) – Efforts to defend against the computer network operations of others, especially those directed against U.S. and allied computers and networks (Source: DCID 7/3).

22. (U) Computer Network Exploitation (CNE) – Unclassified Definition: Intelligence collection and enabling operations to gather data from target or adversary automated information systems or networks. [redacted] (S) [redacted]

[redacted]

23. (U) Computer Network Operations (CNO) – Comprises CNA, CND, and related CNE-enabling operations (Source: DoDD 3600.01).

24. (U) Critical Infrastructure – Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination thereof (Reference u).

25. (U) Cryptologic – Related to the collection and/or exploitation of foreign communications and non-communications emitters, known as SIGINT, and solutions, products, and services to ensure the availability, integrity, authentication, confidentiality, and non-repudiation of national security telecommunications and information systems, known as IA (Source: NSA/CSS Policy 2-12).

(b)(1)
(b)(3)-P.L. 86-36

26. (U) Cybersecurity – As used in this policy, refers to the security of and operations in cyberspace, and encompasses the full range of threat reduction, vulnerability reduction, deterrence international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy, military, and intelligence missions as they relate to the security and stability of the global information and communications infrastructure (Reference ad).

27. (U) Cyberspace – The interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries (Reference d).

(U//~~FOUO~~) 28. ~~(C/~~ [redacted]) Cyberspace Operations – As used in this policy, refers to [redacted]

29. (U) [redacted] P.L. 86-36

(b)(3)-P.L. 86-36

30. (U) DoD Cyberspace Operations – The employment of cyber capabilities where the primary purpose is to achieve objectives in or through cyberspace. Such operations include computer network operations and activities to operate and defend the *Global Information Grid.* (Source: CJCS Memorandum CM-1050-09)

31. (U) Federal Systems – All Federal Government information systems except for National Security Systems of Federal agencies and Department of Defense information systems (Reference d).

32. (U) Global Information Grid (GIG) – The DoD's globally interconnected, end-to-end set of information capabilities for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel. The GIG includes owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services, and National Security Systems.

(b)(1)
(b)(3)-P.L. 86-36

(b)(3)-P.L. 86-3

Non-GIG IT includes stand-alone, self-contained, or embedded IT that is not, and will not be, connected to the enterprise network. (Source: DoDD 8100.01)

(U//~~FOUO~~) 33. (~~C//~~[redacted]) Integrated Cyberspace Operations – As used in this policy, [redacted]

34. (U) Mitigation: As used in this policy, refers to actions taken or activities developed to lessen possible negative outcomes resulting from an equities decision. This may occur when the release of information to support one mission may negatively impact another mission. In this case, actions to lessen the impact must be developed. Alternatively, if release of information is deferred, actions are required to lessen the negative impact that might occur due to the non-release of the information.

35. (U) National Security Systems – Any information system used or operated by an agency, an agency contractor, or other organization on behalf of an agency, where the function, operation, or use of that system involves: intelligence activities; cryptologic activities related to national security; command and control of military forces; equipment that is an integral part of a weapon or weapon system; or is critical to the direct fulfillment of military or intelligence missions; or protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy. (Source: Title 44)

36. (U) Sector-Specific – A Federal department or agency responsible for infrastructure protection activities in a designated critical infrastructure sector or key resources category (Reference o).

(b)(3)-P.L. 86-36

37. (U//~~FOUO~~) Technical Assistance – Including, but not limited to, providing technical knowledge; [redacted]

38. (U) Threat – An adversary having the intent, capability and opportunity to cause loss or damage (Reference af).

(b)(3)-P.L. 86-36

39. (U) United States Cryptologic System – Describes the various U.S. Government entities tasked with a SIGINT mission, i.e., the collection, processing and dissemination of SIGINT, or with an Information Assurance mission, i.e., preserving the availability, integrity, authentication, confidentiality, and non-repudiation of national security telecommunications and information systems.

40. (U) Vulnerability – A technical design or implementation flaw in industrial control systems, government-off-the-shelf, commercial off-the-shelf, or other commercial information

technology products or systems (hardware or software to include open-source software) that permits exploitation or attack by an unauthorized party.

(b)(1)
(b)(3)-P.L. 86-36

(U) ANNEX A

(U) Equities Adjudication

1. (U//~~FOUO~~) This Annex outlines a process for adjudicating NSA/CSS corporate equities. An NSA/CSS corporate equity is an equity that is of interest or importance to more than one NSA/CSS element, and that, if not addressed at a corporate-level, has the potential to adversely affect NSA/CSS's ability to fulfill its SIGINT or IA missions.

2. (U//~~FOUO~~) NSA/CSS corporate equities shall be adjudicated in accordance with existing equities policies.[3] Upon identification of a corporate equity that is not addressed by an existing policy or when parties to an existing policy are not able to reach consensus on the outcome of an equities decision,[4] NSA/CSS elements shall enter into formal equities adjudication in accordance with this annex.

3. (U//~~FOUO~~)

4. (U//~~FOUO~~)

5. (U//~~FOUO~~)

(b)(3)-P.L. 86-36

6. (U//~~FOUO~~) When adjudicating equities, participants shall:

a. (U//~~FOUO~~)

b. (U//~~FOUO~~)

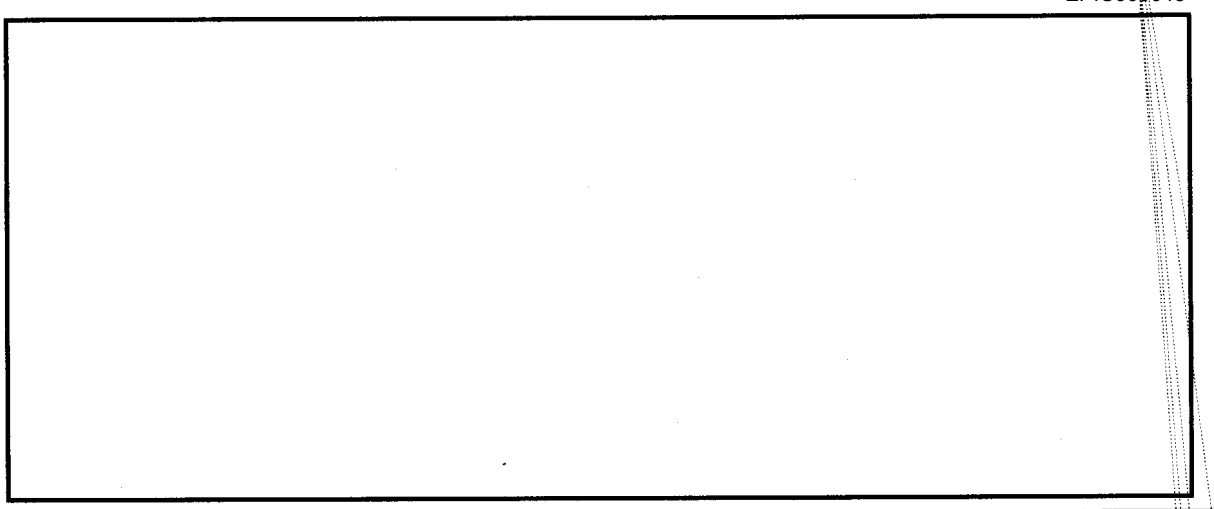
7. (U//~~FOUO~~)

8. (U//~~FOUO~~)

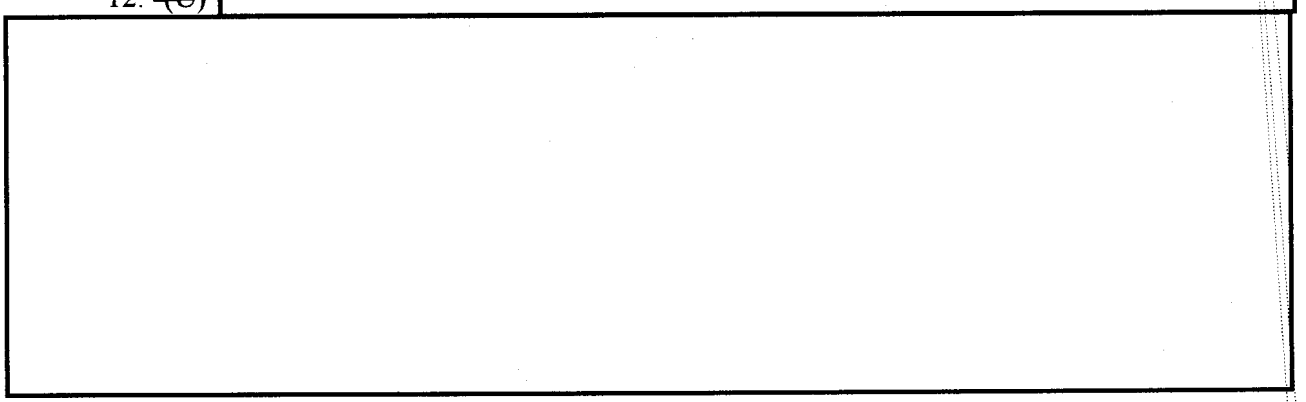
9. (U//~~FOUO~~)

10. (U//~~FOUO~~) An NSA/CSS Equities Adjudicatio n Board (EAB) shall be established to facilitate the adjudication of corporate-level equities and the development of assessment criteria and associated operational deconfliction mechanisms. The EAB shall be apprised upon identification of an equity that is not addressed by an existing equities policy or when parties to an existing equities policy are unable to reach agreement on how to adjudicate a specific instance of an equity. When unable to reach consensus on an issue, the EAB shall elevate it to an NSA/CSS Senior Review Board (SRB) for consideration. An EAB Executive Secretary, with functions that include those described herein, will be established by the SRB.

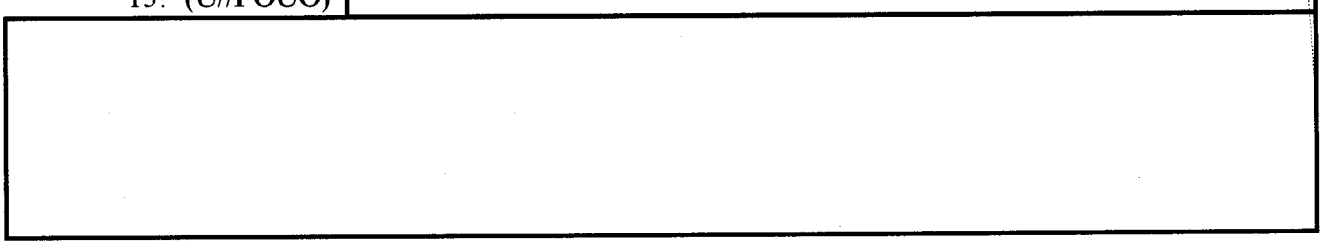
11. (U)



12. ~~(U)~~



13. (U//~~FOUO~~)



14. (U//~~FOUO~~) NSA/CSS equities adjudication deliberations, assessment criteria and associated operational deconfliction mechanisms shall conform to existing laws, policies, and handling procedures, including those governing the information rights and privacy of U.S. persons (References y, z, aa and ab).

15. (U//~~FOUO~~) NSA/CSS elements that invoke an equities adjudication process in accordance with this annex shall comply with the following procedures:

a. (U//~~FOUO~~) Upon identification of a corporate equity for which there is no existing policy, or when parties to an existing equities policy are unable to reach

(b)(3)-P.L. 86-36

consensus on the outcome of a specific equities decision, stakeholders shall notify the NSA/CSS EAB Executive Secretary of the equity issue and of major stakeholders;

b. (U//~~FOUO~~)

c. (U//~~FOUO~~)

d. (U//~~FOUO~~)

e. (U//~~FOUO~~)

f. (U//~~FOUO~~) The NSA/CSS EAB Executive Secretary shall identify and track appropriate metrics related to equities resolution.

[5] This requirement applies to initial adjudication deliberations entered into when there is no existing equities policy or when parties to an existing policy are unable to reach agreement; equities decisions reached through the application of existing equities policies are not subject to this requirement.

(U) ANNEX B

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36

(U) Cryptanalytic Services

(U//~~FOUO~~) NSA/CSS shall provide cryptanalytic services in support of U.S. Government operations in cyberspace as follows (Reference a, b, c, d, e, f and g).

1. (~~S//~~ [redacted]

a. (U//~~FOUO~~) [redacted]

b. (U//~~FOUO~~) [redacted]

c. (U//~~FOUO~~) [redacted]

2. (U//~~FOUO~~) [redacted]

3. (U//~~FOUO~~) [redacted]

a. (U//~~FOUO~~) [redacted]

(b)(3)-P.L. 86-36

1) (U//~~FOUO~~) [redacted]

2) (U//~~FOUO~~) [redacted]

Annex B to Policy 1-58
Dated: 24 March 2011

(b)(1)
(b)(3)-P.L. 86-36

[redacted]

3) (U//~~FOUO~~) [redacted]

[redacted]

4) (U//~~FOUO~~) [redacted]

(b)(3)-P.L. 86-36

[redacted]

b. (U//~~FOUO~~) [redacted]

[redacted]

c. (U//~~FOUO~~) [redacted]

[redacted]