CHAIRMAN OF THE JOINT CHIEFS OF STAFF INSTRUCTION

J-6 CJCSI 6731.01C
DISTRIBUTION: A, B, C 30 October 2010

GLOBAL COMMAND AND CONTROL SYSTEM–JOINT (GCCS-J) SECURITY POLICY

References: See Enclosure D.

1. Purpose. This instruction defines the security policy for the Global Command and Control System–Joint (GCCS-J), its strategic server enclaves, and GCCS–Top Secret (GCCS-T).

2. Cancellation. This instruction supersedes CJCSI 6731.01B CH 1, 30 August 2006.

3. Applicability. See Enclosure A for system identification.

4. Policy. GCCS-J is a U.S. system. Warfighters will be provided GCCS-J security policy consistent with U.S. public laws and policy, DOD information system security policy, automated information system security policy, and defensive information warfare policy, strategy, and doctrine. See Enclosure B for system requirements.

5. Definitions. See Glossary.

6. Responsibilities. See Enclosure C for responsibilities.

7. Summary of Changes. Changes in this instruction clarify security requirements, relationships, roles, and responsibilities pertaining to GCCS-J security.

8. Releasability. This instruction is approved for public release; distribution is unlimited. DOD components (to include the Combatant Commands), other Federal agencies, and the public may obtain copies of this instruction through the Internet from the CJCS Directives Home Page -- http://www.dtic.mil/cjcs_directives.

9. Effective Date. This instruction is effective upon receipt.

CRAIG A. FRANKLIN
Major General, USAF
Vice Director, Joint Staff

ENCLOSURES:

A -- SYSTEM IDENTIFICATION
B -- MINIMUM SECURITY REQUIREMENTS
C -- RESPONSIBILITIES
D -- REFERENCES
GL -- GLOSSARY

TABLE OF CONTENTS

(INTENTIONALLY BLANK)

ENCLOSURE A

SYSTEM IDENTIFICATION

1. Mission Overview. GCCS-J is the Nation's system of record for the command and control of joint and coalition forces. It incorporates the force planning and readiness assessment applications required by battlefield commanders to effectively plan and execute military operations. Its common operational picture (COP) correlates and fuses data from multiple sensors and intelligence sources to provide warfighters the situational awareness needed to act and react decisively. It also provides an extensive suite of integrated office automation, messaging, and collaborative applications. GCCS-J incorporates the latest commercial computer hardware, software, and communications technology. Through an innovative evolutionary acquisition strategy GCCS-J is able to rapidly and cost-effectively field new applications as requirements evolve and technology advances. GCCS-J is fielded at many sites worldwide, all networked via the Department's classified private Intranet. It is designed and implemented to provide our Nation's warfighters the information superiority required to prevail now and well into the 21st century.

2. GCCS-J Definition. Throughout this document, the term "GCCS-J" refers to GCCS-J Global Release, Joint Operation Planning and Execution System (JOPES), Status of Resources and Training System (SORTS) and GCCS-T unless otherwise specified.

3. GCCS-J Classification. GCCS-J is a SECRET-level system. GCCS-T is a TOP SECRET (TS)-level system. GCCS-T provides the capability to transfer focal point (FP) information via Web, news, electronic mail, and secure file transfer protocol. GCCS-T will provide a public key encryption capability to ensure the privacy necessary for FP control. Reference (c) outlines specific procedures for FP.

4. Mission Assurance Category and Level of Confidentiality. The mission assurance category for GCCS-J is Mission Assurance Category I, Classified. This reflects the information handled by the system relative to requirements for integrity (including authentication and non-repudiation) and availability services. The information owner assigned the mission assurance category based on criteria provided in reference (b).

(INTENTIONALLY BLANK)

ENCLOSURE B

MINIMUM SECURITY REQUIREMENTS

1. General Security Policy

a. All GCCS-J information is classified SECRET (TOP SECRET in the case of GCCS-T) until determined otherwise and will be protected per reference f. Security controls will be applied to ensure that GCCS-J systems, applications, and equipment are accessed only by authorized personnel, used only for intended purposes, retain their content integrity, and are marked following reference f. Data owners are responsible for the accurate classification (including releasability markings) of all GCCS-J data to prevent unauthorized access.

b. The security controls selected for GCCS-J will ensure that the system meets the minimum requirements in references a and g. These minimum requirements will be met through automated and manual means in a cost-effective and integrated manner.

c. GCCS-J must meet the requirements established under reference (h). A listing of approved products is available on the National Information Assurance Partnership home page (www.niap-ccevs.org).

d. The interfacing and networking of GCCS-J with a Service or Defense agency information system (IS) must be implemented in accordance with references b and o. Site-designated accrediting authorities (DAAs) may authorize the networking of local area networks (LANs) and ISs with GCCS-J at the appropriate classification level and subject to the restrictions of this security policy.

e. The GCCS-J DAA will issue a type accreditation for GCCS-J releases, supported by the required certification and accreditation (C&A) documentation listed in references a and b. Each site, including combatant command, Service, or agency (C/S/A)–specific versions of GCCS-J, will be provided the “type” C&A documentation to assist in issuing accreditations for those variations of GCCS-J in accordance with reference i. Sites will implement inherited and/or DOD component–specific augmenting IA controls and update enclave accreditation and/or connection documentation to reflect the incorporation/connection of GCCS-J. A separate type-accreditation will be issued for GCCS-T.

f. All changes to type-accredited GCCS-J releases must be reviewed for certification impacts by the Certifying Authority (CA). Changes affecting system functionality and/or security posture will be considered for accreditation by the GCCS-J DAA.

g. Host machines on GCCS-J shall not use standard names indicative of the host’s function. Assigning descriptive names to host machines can give a malicious user valuable information as to the machine’s function (i.e., pop3.GCCSsite.smil.mil is a POP3 mail server) and can aid in developing an attack in the system.

h. Additional guidance for GCCS-T:

(1) GCCS-T is a closed network used for processing TS information.

(2) The SECRET Internet Protocol Router Network (SIPRNET) is the transport mechanism for GCCS-T. GCCS-T data is cryptographically isolated from the SIPRNET using approved TYPE-1 encryption devices. Sites must be connected to their server sites through an approved TYPE-1 encryption device. GCCS-T may only communicate with other TS systems.

(3) DISA/Joint Staff Support Center (JSSC), and the National Security Agency (NSA) will track and control configuration changes to the bulk encryption devices for GCCS-T and will notify the CA and the GCCS-J DAA of any changes affecting system security.

(4) Since GCCS-T is operated as a closed system, sites are prohibited from connecting any other LAN or separate system to GCCS-T without first obtaining written approval from the GCCS-J DAA.

(5) To tightly control expansion of GCCS-T, all requests for new GCCS- T workstations or servers must be approved by the JS/J-3 Deputy Directorate for Global Operations, Command Systems Operations Directorate (DDGO/CSOD). Requests will be copied to the GCCS-J DAA and DISA.

(6) The processing of special handling data on GCCS-T, such as Single Integrated Operational Plan (SIOP) and Special Category (SPECAT), is prohibited under the current type accreditation.

2. General Security Requirements

a. Mobile Code. Reference (j) provides guidance on the implementation of mobile code in DOD information systems.

b. Site Deviations. The site DAA will review/approve requests for deviations to the GCCS-J or GCCS-T baseline configuration and will update the site accreditation documentation accordingly. The site DAA will notify the GCCS-J DAA of any changes that impact overall system security. To ensure proper system functionality and interoperability, the site DAA will not establish more stringent configuration standards than those that have already been approved by the GCCS-J DAA and program manager.

c. Portable Devices. Classified GCCS-J software and data shall not be transferred to unclassified, portable devices. Portable devices, as referenced here, are small hand-held computing devices (excluding laptops) providing personal information management capability for users. If GCCS-J classified information is loaded into an unclassified portable device, the current means for declassification is destruction of the device. Report all incidents involving violation of this requirement to the GCCS-J DAA. Do not destroy equipment involved in security violations until investigation and, if warranted, disciplinary action is complete.

d. Keyboard, Video, Mouse (KVM) Switches. Use of NSA/Central Security Service (CSS) and/or Defense Information Systems Network Security Accreditation Working Group (DSAWG)–approved KVM switches is authorized on GCCS-J with site DAA approval.

e. Web Servers. Any Web server software used by GCCS-J sites will reside on its own physical or virtual device, separated from and independent of other GCCS-J servers. Web server software is defined as any software or system that provides Web content to users or systems outside of the enclave or de-militarized zone (DMZ) where the Web server is located. A server providing a Web portal to users outside the enclave would be considered a Web server. A server providing application services for servers within the same enclave, even if it uses Hypertext Transfer Protocol (HTTP) as its transport, is not considered a Web server.

f. Software. GCCS-J users are prohibited from loading software on GCCS-J workstations and servers without approval from the site DAA.

g. Wireless Technology. The use of wireless technology is prohibited on GCCS-J unless authorized by the GCCS-J DAA and accredited by the GCCS-J DAA or site DAA.

h. Boundary Defense. GCCS-J shall be isolated at each site from the surrounding non-GCCS-J infrastructure by operating the GCCS-J servers on an isolated subnet. All GCCS-J servers will be located in this enclave. It is recommended that GCCS-J clients are also located in the GCCS-J enclave. At a minimum, GCCS-J clients must be located in the local site, post, and/or station enclave.

i. Net-Centricity. GCCS-J will implement data sharing among information capabilities, services, processes, and personnel interconnected within the global information grid (GIG) in accordance with reference o.

j. Enterprise System Management (ESM). ESM is the automation of activities involved in administering, monitoring, operating, and supporting multiple information systems. ESM involves automating repetitive tasks and remotely performing activities that would otherwise be performed by local system administrators. ESM products typically provide automation in one or more of the following disciplines: configuration management, fault management, accounting management, performance management, and security management.

(1) GCCS-J sites may use ESM products that have been approved by the site DAA. Candidate ESM products will be tested for impacts to GCCS-J functionality and security, and the results will be presented to the site DAA for consideration and approval. If the use of SNMP is required, only products supporting SNMP version 3 or later may be considered. DOD-approved ESM capabilities, such as a host-based security system (HBSS), are not subject to the requirement for site DAA approval.

(2) Following site GCCS-J DAA approval, test results will be provided to the GCCS-J DAA. Site DAAs will ensure their respective sites complete all required C&A activities prior to the implementation of ESM

products. As part of this process, the sites will ensure the most recent product service pack/patches are applied and will secure the product using the latest DISA ESM Security Technical Implementation Guide (STIG) and security checklist, and other STIGs and security guides as applicable.

k. Interconnection: The interconnection of GCCS-J with other DOD-component ISs must be supported by a memorandum of understanding (MOU) established between responsible DOD components. The GCCS-J DAA will authorize all such connections.

l. Waivers. All requests for waivers to this instruction must be submitted to the GCCS-J DAA office for approval. Sufficient documentation must accompany all waiver requests and be included in the site certification and accreditation documentation. The requestor shall allow enough time so if the waiver is not approved, an alternate solution can be pursued.

(1) All requests for waivers must be sent in the form of an official memorandum signed by the requesting official. The memorandum should identify the requirement for which the waiver is requested, justification for the waiver, operational impact if the waiver is not granted, description of alternate solutions or procedures that will be implemented in place of the requirement, local points of contact; date by which the waiver is needed, and any supporting documentation that will assist the GCCS-J DAA in making a decision.

(2) Requesting activity must coordinate and receive written endorsement from the user representative, Joint Staff J-3, prior to submitting waiver requests to the GCCS-J DAA.

(3) The GCCS-J DAA, or delegate, will respond, in writing, to all waiver requests.

3. Security Documentation

a. System Documentation. Documentation shall include, at a minimum, security-specific documentation for installation and operation of the system trusted facility manual (TFM), administration of the system, and use of the system Security Features Users' Guide (SFUG). Some applications may require a separate SFUG (e.g., JOPES, SORTS) where the information does not need to be available to all users.

b. Information Assurance Documentation. Documentation shall be developed in accordance with reference (a).

c. Security Classification Guide. A security classification guide shall be created and maintained for GCCS-J.

4. Access

a. Account Access. Access to GCCS-J shall be granted to individuals based on need-to-know and following DOD Regulation 5200.2-R for clearance, special access, and automated data processing category designation requirements and qualifications. GCCS-J user account access is restricted to personnel holding a final U.S. SECRET clearance -- or U.S. TOP SECRET clearance for GCCS-T -- and authorized under references d and e. GCCS-J will operate following the National Disclosure Policy (NDP). Anyone requesting a waiver to the security clearance requirements for GCCS-J or GCCS-T must submit it to the JS/J-3 for approval. The JS/J-3 will forward it to the GCCS-J DAA for review and approval. Contractors must be monitored and activities controlled through appropriate tasking from USG employees, sufficient government oversight as defined and provided by the site, and review of contractor deliverable products.

b. User Identification (USERID). Site GCCS-J program managers and/or system managers shall follow GCCS-J user management requirements as specified in the TFM by establishing a local user management process to assign users a GCCS-J identifier and associate the appropriate roles to that user. GCCS-J shall support user management by providing roles that can perform these actions locally. This includes assigning GCCS-J user identifiers, associating roles within their authority to those user identifiers, and changing passwords per their local process.

c. Individual Identification and Authentication. GCCS-J access is gained through individual identifiers such as Public Key Infrastructure (PKI) credentials. PKI will be used for authentication of identity, access control, non-repudiation, data integrity, and information confidentiality IAW references (b) and (k).

d. Administrative Accounts. The following administrative group accounts within GCCS-J are designed to provide separation of administrative duties: key manager (KEYMAN), system administrator (SA), system administration (SYSADMIN), security manager (SECMAN), and JOPES database manager (JOPESDBA). These accounts enable the establishment of multiple, special-purpose system administrators and thereby enforce the concept of least privilege, especially when used for tasks not requiring full root privilege. The use of these accounts is authorized in conjunction with the following procedures:

(1) GCCS-J sites will limit administrative group account access to authorized system administrators.

(2) In order to ensure auditing capability, direct log-in to an administrative group account that does not uniquely identify an individual administrator is strictly prohibited.

(3) In order to access the accounts identified in paragraph c above, authorized users must first log in using their individual account and then switch user (SU) to the appropriate account.

e. Application/Service Accounts. Application/service accounts are dedicated accounts that create a context for services or applications to run without human interaction. Individual users are prohibited from using application/service accounts to gain access to data. These accounts are not considered group accounts as an individual or group of users will not be able to access data with these accounts. Application/service account passwords must be changed periodically in accordance with the DISA STIGs. If there is a violation of these requirements, the GCCS-J Management Center has the authority to disconnect the interface to protect GCCS-J data and resources.

f. Root Access. GCCS-J sites will limit access and use of root login capability to system administrators only. In addition, GCCS-J sites will maintain accountability of each occurrence when root login is used. The site DAA must authorize the use of root login capability in writing and ensure that the password is only provided to approved system administrators. In order to login as root, authorized administrators must first login using their individual user ID and password and then SU to root. Direct login to root should only be used in emergency situations and during builds.

ENCLOSURE C

RESPONSIBILITIES

1. The Chairman of the Joint Chiefs of Staff (CJCS). The CJCS is responsible for:

a. Providing a security policy that supports user requirements and selected solutions.

b. Identifying minimum system security requirements.

c. Identifying conditions or requirements for entry to various program phases such as operational test, initial operational capability, full operational capability, and system shutdown and termination.

2. The Director for Command, Control, Communications, and Computers (J-6). Joint Staff (JS) J-6, supports the Chairman and the Director for Operations, Joint Staff J-3, in enforcing requirements set forth in this instruction. The Director, J-6, is responsible for:

a. Serving as the principal accrediting authority (PAA) for the warfighting mission area (WMA). Reference a defines general PAA responsibilities.

b. Appointing a DAA.

c. Developing, approving, and maintaining the GCCS-J Security Policy, CJCSI 6731.01.

3. The Director for Operations (J-3). JS J-3 supports the JS J-6 in enforcing the requirements set forth in this instruction. The Director, JS J-3, is responsible for serving as the user representative. Reference (a) defines the user representative role.

4. The Deputy Commander, U.S. Strategic Command. The DCDRUSSTRATCOM serves as the GCCS-J DAA. In addition to the responsibilities defined in references a and b, the GCCS-J DAA responsibilities include:

a. Ensuring GCCS-J complies with assigned security requirements and controls.

b. Authorizing connections to external systems and systems of different security levels. Multi-level security connections also require approval from the DSAWG. Connections between GCCS-T and systems of lower security levels are prohibited.

c. Establishing a GCCS-J security classification guide.

d. Considering waivers to security requirements within this instruction.

e. Chair the C2 Security Working Group with an appropriate O-6–level representative.

f. Developing, implementing, and maintaining security policies and procedures. Publishing amendments and changes to security policies and procedures.

5. Defense Intelligence Agency. DIA serves as the CA for GCCS-J. In addition to responsibilities defined in references a and b, DIA responsibilities include:

a. Serving as the independent type CA for GCCS-J.

b. Validating the minimum set of security requirements for safeguarding GCCS-J information.

c. Conducting IA control validation of GCCS-J type baselines and components.

d. Providing day-to-day GCCS-J, GCCS-T, and strategic server enclave security advice and counsel to the DAA.

e. Independently validating security-relevant baseline changes to GCCS-J configurations, as well as corrections to previously identified security findings.

f. In concert with DISA, assessing and analyzing prototype system configurations for GCCS-J computer security evaluations.

g. Assigning severity categories to all system weaknesses.

6. Defense Information Systems Agency. DISA is the systems integration agent and program manager (PM) for GCCS-J. In addition to responsibilities identified in references a and b, DISA responsibilities include:

a. Implementing security policy.

b. Planning and budgeting for IA controls implementation, validation, and sustainment throughout the GCCS-J system lifecycle.

c. Appointing GCCS-J Information Assurance Managers (IAM) for the type-accredited system baselines (i.e., GCCS-J Global, SORTS, JOPES).

d. Providing centralized security technical support for the development, maintenance, test, evaluation, and use of all components of GCCS-J.

e. In concert with the CA, providing support to the GCCS-J DAA on security of software patches implemented between software releases.

f. Evaluating problem reports and GCCS-J DAA approved change requests for security and providing results, to include system availability issues, to the CA and DAA.

g. Evaluating GCCS-J security incident reports that deal with technical and system software issues and providing analysis and recommendations to the CA and DAA.

h. In concert with the CA, participating in performing IA control validations on standard GCCS-J hardware and software.

i. Developing, installing, analyzing, testing, and evaluating prototype information system security protection systems for GCCS-J with the appropriate C/S/As.

j. Maintaining technical oversight of all aspects of computer network security, including hardware, software, communications security, and emanations security.

k. Evaluating specialized IA tools for use with GCCS-J as requested and approved by the GCCS-J DAA.

l. Providing written mitigation plans for identified findings and vulnerabilities of GCCS-J to the CA and DAA.

m. Evaluating and distributing standard automated software security tools to GCCS-J sites to support implementation of this instruction.

n. Reviewing and providing technical support for security procedures and measures.

o. Providing updates to GCCS-J software in response to emerging security requirements. This includes, but is not limited to, Information Assurance Vulnerability Alerts (IAVAs), JTF-GNO issuances such as Critical Tasking Orders (CTOs), Warning Orders, and vendor bulletins.

p. Ensuring the system certifications support sufficient testing for all hardware, software (OS and applications), and firmware in GCCS-J.

q. Maintaining current vulnerability status for GCCS-J type-accredited baselines in the Vulnerability Management System (VMS).

r. Developing and maintaining the GCCS-J TFMs for the type-accredited baseline.

s. Implement GCCS-J security processes and procedures for the type-accredited system. Participate in the review and updating process for the security policy by providing feedback and comment . .

t. Providing DIACAP documentation to GCCS-J sites for each version or major release of GCCS-J prior to or at the time of installation.

u. Maintain configuration management control of GCCS-J baselines.

v. Implement the GCCS-J security policies and procedures for the type-accredited baselines.

w. Establishing MOAs with PMs/DAAs of connected, external information systems and local DAAs that have connections to external information systems.

7. GCCS-J IAMs. In addition to IAM responsibilities detailed in references a and b, the GCCS-J IAMs (DISA) responsibilities include:

a. Advising CA and DAA on system security matters.

b. Identifying security deficiencies and, where the deficiencies are serious enough to preclude type accreditation, ensuring action is taken to achieve an acceptable security posture or accepting risk.

c. Assisting the GCCS-J PM in implementing the DIACAP.

8. Site-Based Responsibilities

a. Site DAA. The site DAA responsibilities include:

(1) Ensuring site instantiation of GCCS-J complies with assigned security requirements and controls.

(2) Accepting type-accreditation documentation and updating site accreditation based on the acceptability of site-deviations from the type-accredited GCCS-J baseline IAW reference (i).

(3) Ensuring all site-inherited controls, as stated in the GCCS-J accreditation documentation, are implemented and maintained.

(4) Reporting to GCCS-J DAA any site security anomalies that may adversely affect the GCCS-J network or servers.

(5) Ensuring a GCCS-J IAM and information assurance officer (IAO) is appointed in writing for the site; applicable training to carry out the duties of this function is received; and a proper organizational placement is established. (Assigning the site GCCS-J IAM and/or IAO to internal subordinate organizations hampers adequate security accomplishment and is therefore considered a security risk.)

(6) Ensures the site IAMs and IAOs are responsible for ensuring that the site complies with JTF-GNO taskings (i.e. CTOs, warning orders, etc.).

b. Site PM/system manager (SM). Responsibilities include:

(1) Implementing the DIACAP for all GCCS-J systems.

(2) Planning and budgeting for site IA controls implementation, validation, and sustainment throughout the GCCS-J system lifecycle.

(3) Applying approved system updates to GCCS-J software in response to emerging security requirements.

(4) Ensuring GCCS-J system is installed and configured in compliance with applicable security requirements in the TFM, STIGS, etc.

(5) Ensuring annual system reviews required by the Federal Information Security Management Act (FISMA) are conducted.

(6) Ensuring site POA&Ms for GCCS-J are developed, tracked, and resolved.

(7) Appointing a site IAM and/or IAO(s) to assist with security responsibilities, as required.

c. Site IAM. The site IAM is assigned at the discretion of the site/enclave PM/SM for overall security management of single or multiple sites and/or IAOs. Position requires a USG employee in accordance with references p and q. Experience in the application and enforcement of information and IS security measures, threats, and vulnerabilities is essential. Contractor personnel will not fill this position. Responsibilities include:

(1) Implementing security policy and providing security oversight of single or multiple sites and/or IAOs.

(2) Coordinating GCCS-J security measures including analysis, testing, evaluation, verification, accreditation, and review of GCCS-J installation at the appropriate classification level within the site's network structure.

(3) Ensuring security instructions, guidance, and standard operating procedures (SOPs) are prepared and maintained at each site.

(4) Monitoring implementation of security guidance and directing action appropriate to remedy security deficiencies.

d. Site IAO. Reports to the site IAM and/or PM/SM and manages the site GCCS-J security program. Position requires a USG employee or person supervised by a USG employee (i.e. the site IAM) capable of ensuring GCCS-J security policy and guidance in this instruction and other directives have been properly implemented. If the USG employee to whom the IAO directly reports is the appointed site DAA, the IAO is not required to be a USG employee. The IAO is responsible for compliance with GCCS-J security procedures in an assigned area. IAOs may be assigned security responsibility for multiple workstations or areas as long as security is being maintained. If the IAO can logically maintain security control over multiple workstations in different rooms, then the intent of this requirement is met. The site GCCS-J IAO responsibilities include:

(1) Developing, implementing, and managing the site GCCS-J IS security program, to include security education, training, and awareness.

(2) Developing and maintaining the site GCCS-J security policy and procedures.

(3) Coordinating and ensuring site certifications for GCCS-J.

(4) Functioning as the operational arm of the site DAA in implementing and managing the GCCS-J site-approved security processes and procedures.

(5) Acting as the site DAA IS security advisor in the absence of an IAM.

(6) Coordinating all GCCS-J site accreditation submissions and preparing accreditation recommendations for the site DAA.

(7) Monitoring the site GCCS-J equipment usage for unauthorized or improper activity through audit review and intrusion detection.

(8) Supervising and testing all site GCCS-J equipment and software changes.

(9) Investigating and reporting all GCCS-J site security violations to the site DAA, or GCCS-J DAA if outside the site's environment.

(10) Ensuring personnel who use GCCS-J hold proper clearances and that access authorizations are current and valid.

(11) Performing periodic security audits of GCCS-J.

(12) Performing password management.

(13) Ensuring written instructions specifying security requirements and operational procedures exist and are enforced.

(14) Implementing access management and other security-related functions within the scope of their assigned authorities.

(15) Reporting actual or suspected security deviations to the site DAA.

(16) Ensuring the workstations and network interfaces (hardware connections) are physically protected at the remote terminal area to the extent required for the sensitivity of information transmitted through the interfaces.

(17) Collecting and reviewing selected remote facility audit records, documenting any reported problems and corrective actions, and forwarding them to the site DAA.

(18) Promoting security training and awareness.

(19) Acting as the trusted agent (TA) to the local registration authority (LRA) to support GCCS-J users obtaining DOD Public Key Infrastructure (PKI) certificates, in the absence of another PKI TA.

9. GCCS-J User Security Responsibilities. Each GCCS-J user has security responsibilities contributing to the overall operational security of GCCS-J.

GCCS-J users have the responsibility to be aware of and understand GCCS-J security. User responsibilities include:

a. Using the system for only authorized, official purposes.

b. Maintaining individual accountability, ensuring all operations are under assigned user account; not attempting to change or mask assigned user identity; and being responsible for all activity occurring under the assigned user account.

c. Changing access passwords as directed by reference l, following local security SOPs provided by the site GCCS-J IAO. Protecting the SECRET password which authenticates the user by:

(1) Changing account password immediately after the first login.

(2) Not permitting anyone else to use the assigned user account.

(3) Not revealing individual passwords to anyone else at any time.

(4) Storing SECRET passwords in authorized locations and/or containers.

d. Ensuring output products are marked or downgraded and properly safeguarded. Reporting unexpected or unrecognizable output to the site GCCS-J IAO.

e. Not entering data of a higher classification level than the system (SECRET and TOP SECRET for GCCS-T).

f. Protecting classified and other sensitive material. Users will protect all system output (SECRET or TOP SECRET for GCCS-T) until reviewed as to actual classification (based on content) and appropriately downgraded by an approved process. All hardware and output will be marked (labeled) with applicable labels unless properly downgraded. Terminals and workstations located in their respective areas will be safeguarded.

g. Not leaving GCCS-J terminals unattended and signed on.

h. Not moving government-owned hardware or altering communication connections without prior approval from appropriate government local network configuration personnel. Maintaining minimum physical separation of system components following service red/black (TEMPEST) standards.

i. Checking all removable media for viruses before loading on GCCS-J.

j. Complying with all security guidance in this policy and in local security SOPs.

k. Promptly reporting any system security abuses, abnormalities, discrepancies, incidents, vulnerabilities, or any other situation indicating inadequate security to the area security officer and the site GCCS-J IAO.

l. Not attempting to access files or data, or use operating systems, except as specifically designed or authorized.

m. Not installing any hardware or software (including importing or exporting of software). Only system administrators, with the operating in accordance with site policy, can authorize and coordinate installation of additional site-DAA approved software or hardware.

ENCLOSURE D

REFERENCES

a. DODI 8510.01, 28 November 2007, "Department of Defense Information Assurance Certification and Accreditation Process (DIACAP)"

b. DODI 8500.2, 6 February 2003, "Information Assurance (IA) Implementation"

c. CJCSM 3213.02 Series, "The Joint Staff Focal Point (FP) Program"

d. NDP-1, 1 October 1988, "National Policy and Procedures for the Disclosure of Classified Military Information to Foreign Governments and International Organizations"

e. DOD Directive 5230.11, 16 June 1992, "Disclosure of Classified Information to Foreign Governments and International Organizations"

f. DOD Directive 5200.1-R, January 1997, "Information Security Program"

g. DOD Directive 8500.1, 24 October 2002 , "Information Assurance (IA)"

h. National Security Telecommunications and Information Systems Security Policy No. 11, January 2000 and revised June 2003, "National Information Assurance Acquisition Policy"

i. DOD Memorandum, 23 July 2009, "DOD Information System Certification and Accreditation Reciprocity"

j. DODI 8552.01, 23 October 2006, "Use of Mobile Code Technologies in Department of Defense Information Systems"

k. DODI 8520.2, 1 April 2004, "Public Key Infrastructure (PKI) and Public Key (PK) Enabling"

l. DODI 6510.01, 15 August 2007, "Information Assurance (IA) and Computer Network Defense (CND)"

m. CJCSI 3265.01 Series, "Command and Control Governance and Management"

n. Committee on National Security Systems Instruction No. 4009, 26 April 2010, "National Information Assurance Glossary"

o. DOD Directive 8320.02, 23 April 2007, "Data Sharing in a Net-Centric Department of Defense"

p. DOD Directive 8570.01, 15 August 2004, "Information Assurance, Certification, and Workforce Management"

q. DOD 8570.01-M, 20 April 2010, "Information Assurance Workforce Improvement Program"

r. DTM-04-009, 27 September 2004, “Security Classification Marking Instructions,” expires 1 January 2012

s. DTM-04-010, 16 April 2004, “Interim Information Security Guidance,” expires 1 January 2012

GLOSSARY

PART 1 -- ABBREVIATIONS AND ACRONYMS

C

CA	Certifiying Authority
C&A	certification and accreditation
CERT	computer emergency readiness team
C/S/A	Command, Service, Agency
CSS	Central Security Service
CTO	Critical Tasking Order

D

DAA	Designated Accrediting Authority
DADS	Defense Asset Distribution System
DISA	Defense Information Systems Agency
DIA	Defense Intelligence Agency
DIACAP	DOD Information Assurance Certification and Accreditation Program
DOD	Department of Defense
DSAWG	Defense Information Assurance Security Accreditation Working Group

E

ESM	Enterprise System Management

F

FISMA	Federal Information Security Management Act

G

GCCS-J	Global Command and Control System – Joint
GCCS-T	Global Command and Control System – Top Secret
GIG	Global Information Grid

H

HTTP	hypertext transfer protocol

I

IA	information assurance
IAM	Information Assurance Manager
IAO	Information Assurance Officer
IAVA	information assurance vulnerability alert
IAVB	information assurance vulnerability bulletin
IAVM	information assurance vulnerability management

IAV-TA	information assurance vulnerability technical advisory
IAW	in accordance with
IS	information system

J

JOPES	Joint Operations Planning and Execution System
JOPES DBA	JOPES Database Administrator
JS	Joint Staff

K

KEYMAN	key manager
KVM	keyboard, video, mouse

L

LAN	local area network
LRA	Local Registration Authority

M

MOA	memorandum of agreement
MOU	memorandum of understanding

N

NDP	National Disclosure Policy
NSA	National Security Agency

P

PAA	Principal Accrediting Authority
PKI	public key infrastructure
PM	Program Manager

S

SA	system administrator
SECMAN	security manager
SFUG	security features user’s guide
SIOP	single integrated operational plan
SIPRNET	SECRET Internet Protocol Router Network
SM	System Manager
SNMP	simple network management protocol
SOP	standard operating procedures
SORTS	Status of Resources and Training System
SPECAT	special category
STIG	Security Technical Implementation Guide
SU	switch-user
SYSADMIN	system administration

	T
TFM	trusted facility manual
TA	Trusted Agent
	U
U.S.	United States
USERID	user identification
USG	United States Government
USSTRATCOM	United States Strategic Command
	V
VMS	Vulnerability Management System
	W
WMA	warfighting mission area

PART II -- DEFINITIONS

See reference n for the definitions of IA terms used in this instruction.