United States Cyber Command Instruction (USCCI)

OPR: J070
DISTRIBUTION: B

USCCI 5900-04
2 December 2016

Classification Advisory Officer Program

1. Purpose. This U.S. Cyber Command (USCYBERCOM) Instruction (USCCI) establishes policies, procedures, requirements and responsibilities for the USCYBERCOM Classification Advisory Officer (CAO) Program.

2. Supersedes/Cancellation. This Instruction supersedes USCCI 5900-04, *Classification Advisory Officer Program,* dated 11 Jan 2011.

3. Applicability. This Instruction applies to all USCYBERCOM personnel assigned to Headquarters (HQ) USCYBERCOM, and its subordinate units, to include HQ Cyber National Mission Force, the Service Components, the Joint Force Headquarters-Cyber, the Joint Force Headquarters – Department of Defense Information Networks, and designated Joint Task Forces, which are hereby referred to as the USCYBERCOM enterprise, that produce and classify information and protect Controlled Unclassified Information.

4. Responsibilities. Responsibilities are outlined in Enclosure 1.

5. Procedures. Procedures are outlined in Enclosure 2.

6. Releasability. Cleared for Public Release. This Instruction is approved for public release; distribution is unlimited. Department of Defense (DoD) Components, other Federal agencies and the public may obtain copies of this directive.

7. Summary of Changes. This instruction has been substantially revised and must be completely reviewed. Significant changes include the following:

a. The preponderance of CAO training now occurs via on-line courses versus instructor-led classroom instruction.

b. The extension of the USCYBERCOM CAO Program to include the Components.

c. The addition of Directorate/Component Lead CAOs, with focus on conducting self-assessments of classified information products.

d. The addition of qualifications or status to serve as a CAO.

e. The addition of roles and responsibilities for Derivative Classifiers.

f. The expansion of the metrics and self-inspection requirements.

8. Effective Date. This Instruction is effective immediately upon receipt.

STEPHEN G. FOGARTY
Major General, USA
Chief of Staff

Enclosures:
ENCLOSURE 1 – Roles and Responsibilities
ENCLOSURE 2 – Policies and Procedures
ATTACHMENT 1 – Glossary of References and Supporting Information

ENCLOSURE 1

1. Roles and Responsibilities.

1.1. Chief of Staff (CoS).

1.1.1. Administer the CAO program for the Command and Components. At a minimum, the CAO program directs the Services to provide security classification training (this is provided through the Defense Security Service (DSS)) to USCYBERCOM and its Components. All USCYBERCOM enterprise personnel must comply with security classification guides (SCG) and directives, and pertinent DoD and U.S. Government orders, directives, instructions, and regulations creating and governing information security classification programs.

1.1.2. Appoint a Chief CAO, and a Deputy Chief (D/Chief) CAO in writing and certify them as trained and qualified to perform CAO responsibilities and manage all aspects of the CAO program.

1.2. Chief CAO.

1.2.1. Receive appointment in writing from the CoS and be certified as trained and qualified to perform Chief CAO duties upon completion of the Center for Development of Security Excellence (CDSE) courses as specified in the training section.

1.2.2. Manage all aspects of the CAO program.

1.2.3. Maintain this instruction and USCCI 5200-03, *Security Classification Guide*, and refer to relevant classification guidance when applicable.

1.2.4. Possess the following qualifications or status:

1.2.4.1. Current in terms of the completion of the previously instructed USCYBERCOM CAO course, or the newly adopted CAO training courses available at the DSS, CDSE or equivalent training courses as determined by the Chief CAO, as specified in the training section below.

1.2.4.2. Working knowledge of USCYBERCOM and related SCGs.

1.2.4.3. Be a military member or government civilian employee.

1.2.5. Serve as the Command's senior classification subject matter expert (SME) and senior derivative classifier. Retain final authority within the Command to resolve derivative classification questions. Resolve classification questions involving original classification issues by consulting with and advising the Command's Original Classification Authorities (OCA).

1.2.6. Provide expert classification marking system advice. Manage the classification program in support of the OCA in accordance with (IAW) Executive Order (E.O.) 13526, *Classified National Security Information*; Information Security Oversight Office (ISOO) 32 CFR Part 2001 and 2003 Classified National Security Information, *Final Rule*; USCCI 5200-03, *Security Classification Guide*; Intelligence Community Directive (ICD) 710, *Classification Management and Control Marking System*; Office of the Director of National Intelligence (ODNI), *Intelligence Community Markings System Register and Manual*; DoD Manual (DoDM) 5200.45, *Instructions for Developing Security Classification Guides*; and source documents.

1.2.7. Comply with all classification program oversight and reporting requirements including preparing annual reports and conducting program reviews and inspections.

1.2.8. Maintain current knowledge of national and DoD classification policy and regulation changes and disseminate new information to the USCYBERCOM enterprise.

1.2.9. Identify and verify Command requirements for OCA, and work with DoD Classification Program authorities to have OCA delegated within the Command.

1.2.10. Identify the specific CDSE, or equivalent, courses required to be qualified as a USCYBERCOM CAO.

1.2.11. Meet regularly with all Command CAOs for networking, disseminating information about new and emerging classification issues, and identifying and resolving any new classification issues within the USCYBERCOM enterprise.

1.2.12. Require quarterly self-assessment spot checks from all USCYBERCOM enterprise Lead CAOs. Aggregate the information, and provide to the USCYBERCOM Chief Knowledge Officer (CKO) a summary of the quarterly spot checks to provide a status on the state of the classification program.

1.2.13. IAW direction from the CoS, review, verify and validate self-assessments and self-inspections conducted by each Directorate/Component on a quarterly basis, and provide an aggregate summary of discrepancies to the CoS with recommendations for mitigation.

1.2.14. Submit the Standard Form 311, *Agency Security Classification Management Program Data*, and the *Agency Annual Self-Inspection Program Data* report to the Office of the Under Secretary of Defense for Intelligence, the ISOO and HQ United States Strategic Command.

1.3. D/Chief CAO.

1.3.1. Receive appointment in writing from the CoS and certification as trained and qualified to perform D/Chief CAO duties.

1.3.2. Assist the Chief CAO with the management of all aspects of the CAO program.

1.3.3. Possess the following qualifications or status:

1.3.3.1. Current in terms of the completion of CAO training, as specified in the training section below.

1.3.3.2. Working knowledge of USCYBERCOM and related SCGs.

1.3.3.3. Be a military member or government civilian employee.

1.3.4. When developing SCGs for the command, ensure they comply with DoDM 5200.45.

1.4. USCYBERCOM Enterprise Directors and Commanders.

1.4.1. Implement a CAO program within their organizations.

1.4.2. Nominate personnel for CAO training and designation. The Chief CAO designates all CAOs. Certification of training and nomination from leadership are required for designation.

1.4.3. Maintain a sufficient number of CAOs to meet all classification review requirements under their purview in a timely manner.

1.4.4. Designate a Lead CAO to serve as the point of contact (POC) to the Chief CAO.

1.4.5. Ensure all derivative classifiers and personnel who have access to classified material are evaluated on their performance in classifying, safeguarding and handling classified material per E.O. 13526.

1.4.6. Oversee self-assessments and self-inspections. Based on the results, improve processes impacting the production and marking of classified materials and documents.

1.5. USCYBERCOM Enterprise Lead CAOs.

1.5.1. Provide guidance and awareness of the CAO program to their organization's personnel. Confirm those who create and classify information do so IAW USCCI 5200-03 and other applicable SCGs, regulations and instructions.

1.5.2. Conduct their organization's self-assessment of information products, as required by the Chief CAO, to determine if they conform to standing requirements for classified information IAW the USCYBERCOM Information Security and Classification Standard Operating Procedures (SOP), available in separate correspondence, in conjunction with the ISOO 32 CFR Part 2001 and 2003 Classified National Security Information and DoDM 5200.01 Volumes 1-4, *DoD Information Security Program.*

1.5.3. Ensure all personnel log/track derivative classification actions on serial/finished products and provide required metrics on an annual basis as specified by the Chief CAO IAW the USCYBERCOM Classification SOP (separate correspondence).

1.5.4. Maintain a tracking mechanism for the training status of their organization's CAOs. Coordinate with and ensure leadership designates enough CAOs to support mission requirements.

1.5.5. Direct classification advisory tasks to their organization's CAOs.

1.5.6. Provide self-assessment and self-inspection reports on their organization's activities and status of CAOs to the Chief CAO, upon request.

1.6. CAOs.

1.6.1. Maintain certification as trained and qualified to perform CAO duties.

1.6.2. Provide classification advice, assistance and recommendations to document owners within their organization, using the appropriate SCGs and Classification SOPs IAW DoDM 5200.01 Volumes 1-4 and USCCI 5200-03. Ensure document owners identify the classifier, derivative classification sources, and declassification date in a classification authority block. NOTE: CAOs are not responsible for classifying and marking documents on behalf of the document owner. It is the document owner's responsibility. However, the document owner cannot execute the CAO review for his/her own documents.

1.6.3. Possess the following qualifications or status:

1.6.3.1. Current in terms of the completion of the previously instructed USCYBERCOM CAO course, or the newly adopted CAO training courses available at the CDSE or equivalent training courses, as specified in the training section below.

1.6.3.2. Working knowledge of USCYBERCOM and related SCGs.

1.6.3.3. Be a military member or government civilian employee.

1.6.4. Conduct classification reviews to verify correct classification and marking of documents when requested, or as required in this USCCI. Report review findings to the document owner, and advise the document owner on how to make necessary classification and marking changes IAW DoDM 5200.01 Volumes 1-4, ICD 710 and ODNI Intelligence Community (IC) Markings System Register and Manual.

1.6.5. Work collaboratively and consult with operational, technical, and administrative SMEs as needed to ensure consistent, high quality classification expertise and solid CAO determination recommendations.

1.6.6. Ensure all cleared derivative classifiers working within their organization track the number of documents created annually for each classification level.

1.6.7. Advise all personnel on the proper procedures and resources to secure and handle classified materials.

1.6.8. Work within their organization to meet CAO requirements as specified by their respective Lead CAO's direction.

1.7. Derivative Classifiers.

1.7.1. Make derivative classification determinations based on the standing OCA decisions that have been documented in writing, specifically in SCGs, memorandums, and source documents. Take the appropriate introductory and follow-on classification training, be a recognized SME in the field of study in which classification determinations are being considered, and be consistent with the OCA SCG.

1.7.2. Complete initial classification training within 60 days of arrival, and maintain currency with the annual classification training as specified in the training sections below.

1.7.3. Properly classify information IAW the respective OCA SCGs, and safeguard classified information IAW DoDM 5200.01. Consult with the respective CAOs and review their documents to ensure proper format, portion marking, banners, and classification authority blocks with declassification dates.

1.7.4. Track classification determinations as appropriate to accurately capture the number of classified documents created at the CONFIDENTIAL, SECRET, and TOP SECRET levels, and provide to the respective lead CAO for aggregation within each organization.

1.7.5. Use guidance from other organizations that have purview when there is a lack of USCYBERCOM classification guidance on a topic. For example, the USCYBERCOM SCG does not address Signals Intelligence. If the appropriate organization has similar or relevant classification guidance, reference that guidance for the classification determinations, and reference those SCGs in the classification authorities' block.

1.8. Document Owners.

1.8.1. Properly classify documents, and safeguard the handling and transmission or transportation of these documents to and from Sensitive Compartmented Information Facilities (SCIF). Document owners are the creators of documents containing information from sources and methods that require protection based upon the guidance of the OCA. Documents consist of unclassified, controlled unclassified, and/or classified information. The CAOs in an organization should not be the document owners, and should be considered advisors to the document owners. Document owners should use best practices by developing a process for the creation of documents that includes a CAO review of the information and classification markings to ensure compliance with command instructions.

1.8.2. Ensure that all classified material has the appropriate portion markings, banners, classification authority block with the proper identifier of the derivative/original classifier, source of classification guidance, or source document (in the case of multiple sources, references spelled out in the document) and declassification date. Take responsibility for any spillage of documents. Resolve potential security violations, spillage (see Committee on National Security Instructions (CNSSI) No. 1001, *National Instruction on Classified Information Spillage*), and/or compromises in cooperation with security personnel IAW DoDM 5200.01 Volumes 1-4, Deputy Secretary of Defense (DepSecDef) Memorandum, *Unauthorized Disclosure of Classified Information or Controlled Unclassified Information on DoD Information Systems*, and Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01B, *Cyber Incident Handling Program.*

1.8.3. Correct the classification of a document based on CAO recommendations for classification of documents. Garner CAO review approval, when required.

1.9. Services.

1.9.1. Provide information security training to all personnel across the USCYBERCOM Enterprise. CAO training and other information security topics are to be provided by the Services, which have designated the DSS, CDSE as the primary provider of such training via on-line courses. See the training requirements below for the CAO program. USCYBERCOM is not responsible for providing such training and is not manned nor prepared to support such training requirements. The services need to ensure their personnel within the USCYBERCOM enterprise are properly trained to perform CAO duties.

1.9.2. The Chief CAO is available to interpret and validate the CDSE training meets USCYBERCOM requirements.

ENCLOSURE 2

2. Policies and Procedures.

2.1. Classification Review Process.

2.1.1. Document Owners.

2.1.1.1. Document owners are mandated to classify and mark their documents such as reports, orders, power point presentations and e-mails when originally created using the USCCI 5200-03 and other applicable SCGs. Document owners are encouraged to seek assistance and advice from a CAO, when necessary.

2.1.1.2. Document owners are responsible for requesting a classification review from a CAO as specified in this USCCI. Document owners must include the name or identifier of the derivative classifier that created the document, so the system, in case of classification challenges, can track down that individual to determine if they followed the proper procedures. Dates of the classification guides are necessary to ensure the derivative classifiers are following the proper guidance. Declassification dates are needed for the timeframe considered necessary to ensure proper protection of information as well as sources and methods.

2.1.2. CAOs.

2.1.2.1. Before conducting a classification review, CAOs must obtain the name of the individual initially responsible for classifying the document in question. The CAOs must consult with that individual, document owners, and content SMEs to resolve classification questions.

2.1.2.2. The CAOs check the classification marking of the document; ensuring standards are met IAW DoDM 5200.01 and the ODNI IC Markings System Register and Manual. The CAOs consult the document owner, SMEs, and other CAOs, as necessary, to answer any questions that arise during the review. Getting consensus among the experts provides due diligence and ensures the information is properly classified and protected. CAOs should use the best practices of logging their decisions and ensuring proper documentation of their recommendations to document owners so the CAO is protected and prepared to defend their determinations if questions subsequently arise.

2.1.2.3. The CAOs report the results of the review to the document owner, and advise the owner on how to make corrections to the documents. The CAO is not responsible for making the corrections on behalf of the owner.

2.1.2.4. When requested to confirm a document's classification level before moving it between networks of differing classification levels, the CAOs must confirm their review results in writing, or by a digital signature email. The CAOs review the information and determine whether the document transfer to the intended destination network is consistent with the Data Transfer Authority instructions and policies (see Command Policy Memorandum (CPM) 2011-19, *Interim Data Transfer Authority Policy and Procedures*.

2.2. Training.

2.2.1. The Chief CAO refines and maintains CAO training requirements, and either leverages CDSE courses available on-line at www.cdse.edu/catalog/elearning/index.html (see Section 2.5.5 for the list of identified courses for CAO qualification) or equivalent courses to be completed no later than the three year anniversary of attaining the current CAO certification.

2.2.2. The Chief CAO may still teach platform CAO training classes as directed, and/or hold classification advisory workshops with the USCYBERCOM enterprise. For instructor led training, the requirements must be external to the Command, subject to the availability of funds and instructors; held at a proper SCIF with a classroom with appropriate media and sound equipment to present information to students; and at no cost to USCYBERCOM. The CDSE courses will form the primary basis of the training.

2.2.3. IAW E.O. 13526, the Chief CAO either develops or identifies a suitable curriculum for classification refresher training and ensures that all USCYBERCOM enterprise personnel who create derived classified information/materials receive refresher training annually.

2.2.4. IAW E.O. 13526, the Chief CAO also develops and maintains a curriculum for OCA refresher training and provides that training to the OCAs as required. Only two USCYBERCOM senior leaders retain OCA (see DepSecDef Memorandum, *Delegation of Top Secret (TS) Original Classification Authority (OCA)*). The Chief CAO provides annual training for the Deputy Commander, USCYBERCOM. In the event additional personnel are delegated OCA, they are required to take the annual OCA refresher training.

2.2.5. All CAOs will review this instruction annually to maintain cognizance of applicable policies, responsibilities, and procedures, as well as keep abreast of any changes that may be promulgated.

2.2.6. All personnel should complete their initial classification training within 60 days of assignment to HQ USCYBERCOM or a Component, respectively.

2.2.7. Derivative Classifiers are required to take annual derivative classification training via the CDSE Security Training, Education and Professionalization Portal (STEPP) IF103.16, *Derivative Classification Course* or an equivalent course.

2.3. Resources.

2.3.1. The Chief CAO maintains an electronic library of current SCGs, policies, instructions, and regulations relevant to the USCYBERCOM enterprise, and ensures it is accessible to all personnel. The Chief CAO distributes an appropriate link to the CAOs. The

Chief CAO will work with Knowledge Management to make the library accessible across the USCYBERCOM enterprise.

2.3.2. The Chief CAO maintains a current roster of CAOs, and publishes that roster for access by all USCYBERCOM enterprise personnel via an appropriate link distributed to the CAOs. Lead CAOs need to provide status updates on the training status of CAOs within their organization and provide periodic updates to the Chief CAO, as requested.

2.3.3. The Chief CAO refines and maintains an overarching USCYBERCOM SCG for signature by either of USCYBERCOM's OCAs. The Chief CAO maintains the SCGs IAW E.O 13526 and DoDM 5200.45, and retains copies of the relevant references in the USCYBERCOM share drives.

2.4. Metrics and Record Keeping.

2.4.1. All CAOs will maintain classification review records as directed in writing by the Chief CAO. CAOs must track their actions as a CAO, and log when they make classification determinations, and when they exercise derivative classification. See the Chief CAO for an example of an activity log. The log can be a spreadsheet or some mechanism used to capture security classification actions by date, context, and POCs. An example will be made available in the Classification SOPs.

2.4.2. The Chief CAO will regularly collect classification review metrics and report them to the USCYBERCOM CoS, and CKO, as needed.

2.4.3. All lead CAOs will maintain a record of Self-Assessment Spot Checks or self-evaluations and provide their respective reports to their leadership and the Chief CAO. Self-Assessment Spot Checks will consist of a review of between five to twenty individual documents of at least one page/slide/thread, and a marking up of potential discrepancies based off standing ISOO criteria. Based on any noted deficiencies in these documents, the Lead CAOs will provide recommendations to correct these errors, and to curtail similar discrepancies in the future to their leadership and the Chief CAO. Additional guidance will be provided via separate correspondence and in a Classification SOP that will be produced separately from this USCCI.

2.4.4. All CAOs will remind derivative classifiers to maintain a log of their derivative classification actions. The requirement is to collect the number of derivative classification actions per classification level. Such activity logs need to be updated, and available for self-inspection and program reviews.

2.5. Certification and Designation.

2.5.1. All CAOs must have at least two years' experience in handling and protecting classified information. As classification is an inherently governmental function per E.O.13526, CAOs must be military members or government civilians assigned within the USCYBERCOM enterprise. Governmental contractors may complete CAO training and provide advice, but they cannot sign off on CAO activities.

2.5.2. All USCYBERCOM and Component CAOs must complete/pass the USCYBERCOM CAO designated courses from CDSE, as specified in the training section above, to be qualified as a CAO. Only USCYBERCOM affiliated personnel can be designated as a USCYBERCOM CAO. The Chief CAO designates all CAOs. Certification of training and nomination from leadership are required for designation. The Chief CAO will determine what courses from other organizations are accepted as equivalent to the CDSE courses.

2.5.3. All USCYBERCOM CAOs must recertify every three years, which includes retaking select CDSE CAO Courses (see Section 2.5.5), or equivalent courses. Upon completion, the training statuses of CAOs are updated as renewed.

2.5.4. USCYBERCOM CAOs may complete Virtual University Port courses for professional development, but they will not be used for certification.

2.5.5. The following CDSE courses are required for the initial CAO qualification. The courses marked with an '*' are the minimum CDSE courses required to recertify as a CAO at the three year mark. The courses available via STEPP are as follows:

1) IF103.16*, *Derivative Classification Course*, 14 April 2016.
2) IF110.06, *Classification Conflicts and Evaluations Course*, 2 March 2015.
3) IF011.16*, *Introduction to Information Security Course*, 27 August 2015.
4) IF105.16*, *Marking Classified Information Course*, 27 August 2015.
5) IF102.16, *Original Classification Course*, 27 August 2015.
6) IF101.16, *Security Classification Guidance Course*, 12 June 2015.
7) IF107.16, *Transmission and Transportation for DoD Course*, 12 June 2015.
8) IF130.16, *Unauthorized Disclosure of Classified Information for DoD and Industry Course*, 12 June 2015.

2.6. Data Spillage/Security Violations.

2.6.1. Data spillage (see CNSSI No. 1001) occurs when classified information, whether properly or improperly marked, is observed on a network not approved to hold that level of classified information. When data spillage occurs, the local CAO must inform the document/content owner of their determination whether the information purportedly compromised was classified or not.

2.6.1.1. The document/content owner must immediately notify all personnel in possession of the information that it is classified or improperly classified, resides on the wrong network or medium, and is not to be disseminated further. Appropriate clean up procedures will follow.

2.6.1.2. The local CAO conducts a review and validates the classification of the information. The document/content owner submits evidence for incident handling per local security procedures and informs leadership to rectify any security considerations.

2.6.1.3. The document/content owner is responsible for reporting the spillage, and any other potential security violations (see DoD Directive (DoDD) 5210.50, *Management of Serious Security Incidents Involving Classified Information*, and USCCI 5200-08, *Information Assurance (IA) Policy*), to the Command Special Security Officer (SSO)/Security Chief, and complying with all instructions from the SSO/Security Chief.

2.6.1.4. Cybersecurity incident handling procedures are found USCCI 5200-08.

2.7. Required CAO Reviews.

2.7.1. A CAO review may be requested at any time, but is mandated in the following circumstances:

2.7.1.1. Prior to transfer of a document to a network with a lower classification level.

2.7.1.2. Prior to release of a document intended for public use.

2.7.1.3. Prior to release of an official document for use with external organizations. It is imperative that a CAO review is done prior to sharing official documents with external organizations. It is a matter of professionalism and accuracy, and minimizes any classification challenges. Furthermore, it aids the future handling of the information/documents as they progress through their life cycle and are subject to Freedom of Information Act requests, declassification, disclosure, and release.

2.7.2. The Chief CAO must review major policy documents produced by the Command.

2.7.3. A CAO review is not required for routine documents kept within an organization, or handled as part of an organization's normal business routine. In those cases, document owners are responsible for correct classification and marking and should seek assistance from a CAO when needed. Document owners will properly mark all documents IAW Command policies, ensuring portion marking, banners, and classification authority blocks and declassification dates.

2.7.4. A CAO review is not required for documents that are under development or in draft form. However, personnel working with such documents are responsible for protecting them at an appropriate security level regardless of the state of their classification markings.

2.7.5. When CAO review is required for sharing with foreign partners, such reviews need to be conducted prior to the Foreign Disclosure Officer, and/or Foreign Disclosure Release Officers. The review will ensure any foreign disclosure actions are compliant with SCGs and the National Disclosure Policy Manual 1 (NDP-1).

2.8. Staffing Process.

2.8.1. The document owner must ensure proper classification of all finished documents. Documents routing outside of the USCYBERCOM enterprise require proper staffing. A CAO review will occur prior to action officer level approval. Any recommendations should be addressed by the document owner before the CAO concurs/signs off the review as complete.

2.8.2. When substantive changes to a document occur in later stages of staffing, a second CAO review is appropriate prior to General Officer/Flag Officer approval.

ATTACHMENT 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

E.O. 13526, *Classified National Security Information*, December 29, 2009

ISOO, *32 CFR Part 2001 and 2003 Classified National Security Information; Final Rule*, effective June 25, 2010

DoDM 5200.01 Volumes 1-4, *DoD Information Security Program*, 24 February 2012, as amended

USCCI 5200-03, *Security Classification Guide*, 15 April 2015

ICD 701, *Security Policy Direction for Unauthorized Disclosure of Classified Information*, 14 March 2007

ICD 710, *Classification Management and Control Marking System*, 21 June 2013

ODNI, *Intelligence Community Markings System Register and Manual*, 24 December 2015

DoDM 5200.45, *Instructions for Developing Security Classification Guides*, 2 April 2013

DepSecDef Memorandum, *Unauthorized Disclosure of Classified Information or Controlled Unclassified Information on DoD Information Systems*, 14 August 2014

CJCSM 6510.01B, *Cyber Incident Handling Program*, 10 July 2012

DoDD 5210.50, *Management of Serious Security Incidents Involving Classified Information*, 27 October 2014

CNSSI No. 1001, *National Instruction on Classified Information Spillage*, February 2008

USCCI 5200-08, *Information Assurance (IA) Policy*, 4 February 2014

DepSecDef Memorandum, *Delegation of Top Secret (TS) Original Classification Authority (OCA)*, 3 February 2011

USCCI 5000-01, *Correspondence Management*, 22 April 2016

National Disclosure Policy Manual 1 (NDP-1), 2 October 2000

CPM 2011-19, *Interim Data Transfer Authority Policy and Procedures,* 18 Jan 2012

Acronyms & Abbreviations

CAO – Classification Advisory Officer
CDSE – Center for Development of Security Excellence
CJCSM – Chairman of the Joint Chiefs of Staff Manual
CKO – Chief Knowledge Officer
CNSSI – Committee on National Security Instructions
CoS – Chief of Staff
D/Chief – Deputy Chief
DepSecDef – Deputy Secretary of Defense
DoD – Department of Defense
DoDD – Department of Defense Directive
DoDM – Department of Defense Manual
DSS – Defense Security Service
E.O. – Executive Order
HQ – Headquarters
IA – Information Assurance
IAW – in accordance with
IC – Intelligence Community
ICD – Intelligence Community Directive
ISOO – Information Security Oversight Office
NDP-1 – National Disclosure Policy-1
OCA – Original Classification Authority
ODNI – Office of the Director of National Intelligence
POC – Point of Contact
SCG – Security Classification Guide
SCIF – Sensitive Compartmented Information Facility
SME – Subject Matter Expert
SOP – Standard Operating Procedure
SSO – Special Security Officer
STEPP – Security Training, Education and Professionalization Portal
USCCI – United States Cyber Command Instruction
USCYBERCOM – United States Cyber Command

Supporting Information:

UNCLASSIFIED CDSE Web Site
www.cdse.edu/catalog/elearning/index.html