EFFECTIVE DATE

(03-27-2020)

PURPOSE

(1) This transmits revised CCDM 30.6.1, Security and Emergency Preparedness; Security of Confidential Information, Official Documents, Tax Data, Personnel and Property.

MATERIAL CHANGES

(1) CCDM 30.6.1.2.3, Electronic Mail and Messaging, is revised to reflect updated IRM references and messaging technology available to Chief Counsel employees, as well as a new section (4) setting forth encryption requirements for sending email messages or attachments to recipients outside the IRS.

(2) CCDM 30.6.1 - updated the links and references throughout the document.

EFFECT ON OTHER DOCUMENTS

This section supersedes CCDM 30.6.1.2.3, Electronic Mail and Messaging, dated October 5, 2016..

AUDIENCE

Chief Counsel

Thomas J. Travers
Associate Chief Counsel
(Finance and Management)

30.6.1
Security of Confidential Information, Official Documents, Tax Data, Personnel and Property

Table of Contents

30.6.1.1 Policy and Guidelines
30.6.1.1.1 Security of Information, Documents, and Property
30.6.1.1.2 Security Responsibilities
30.6.1.2 Security of Confidential Information, Official Documents and Tax Data
30.6.1.2.1 Documents Classified as ″Official Use Only″
30.6.1.2.2 Disposition of SBU and OUO Information
30.6.1.2.3 Electronic Mail and Messaging
30.6.1.2.4 Records Statutes, Records Control Schedules and Disclosure
30.6.1.3 Security of Personnel and Property
30.6.1.3.1 Identification Media
30.6.1.3.2 Protection Standards
30.6.1.3.3 Access Control
30.6.1.3.4 Mail Handling
30.6.1.3.4.1 Mail Delays

30.6.1.1
(01-30-2008)
Policy and Guidelines

(1) This section establishes policies and guidelines for the security of information, documents, personnel, and property in the Office of Chief Counsel.

(2) Security management and procedures will be determined by the Associate Chief Counsel (Finance & Management) in his/her role as the Designated Accrediting Authority (DAA), using the following as guidance after taking into account the risks and needs of the Office of Chief Counsel:

- The Privacy Act of 1974
- Federal Information Security Management Act (FISMA) of 2002
- OMB Circulars A-123 and A-130
- Treasury IT Security Program, TDP 85-01
- Federal Information Processing Standards (FIPS)
- Public Law 105-93

(3) Additionally, such procedures will be consistent with the provisions of IRC sections 6103, 7213, 7217 and 7431.

30.6.1.1.1
(01-30-2008)
Security of Information, Documents, and Property

(1) Employees are responsible for the protection and proper disposition of all information, documents and property in their possession or control. They must make every effort to protect information, documents and other property entrusted to their care and prevent unauthorized entry into areas where the information, documents and property are located.

(2) The guidelines included in this section are applicable to employees working in flexiplace locations. Files containing IRS information or data will be secured when not in use or in the possession of the employee.

(3) For guidelines concerning Chief Counsel and IRS information systems, employees should consult their servicing MITS organization or IRM 10.8.1, Information Technology (IT) Security Policy and Guidance.

30.6.1.1.2
(03-29-2006)
Security Responsibilities

(1) The responsibilities of managers are to:

- Support safety and security programs and policies
- Ensure adequate training of personnel in safety and security (e.g., fire drills)
- Discuss safety and security procedures with employees at least annually
- Ensure security measures are followed to protect life, information, facilities, and property within their areas

(2) The responsibilities of employees are to:

- Support safety and security programs and policies
- Report accidents or incidents promptly
- Assist in the investigation and removal of hazards
- Be alert to strangers or suspicious packages in the work area

30.6.1.2
(04-29-2009)
Security of Confidential Information, Official Documents and Tax Data

(1) Sensitive But Unclassified (SBU) information is defined as any information that requires protection due to the risk and magnitude of loss or harm to the IRS or the privacy to which individuals are entitled under 5 U.S.C. (§) 552a (the Privacy Act), which could result from unintentional or deliberate disclosure, alteration or destruction.

(2) SBU shall be the primary term used to mark sensitive but unclassified information originating within Chief Counsel offices. The SBU designation identifies information that, if released, could cause harm to a person's privacy or welfare; adversely impact economic, industrial, or international financial institutions; or compromise unclassified programs, essential operations or critical infrastructures. The "Official Use Only" and "Limited Official Use" designations, which are solely used to prevent the automatic distribution to the public of printed materials, should not be routinely used to identify SBU information contained in Office of Chief Counsel documents. For assistance in these matters, contact Branch 6 or 7 of the office of the Associate Chief Counsel (Procedure & Administration).

Note: Although information that would be required to be disclosed under the Freedom of Information Act (FOIA) generally should not meet the criteria for SBU designation, simply because information bears the SBU designation does not mean it is automatically exempt from the FOIA. SBU information that becomes the subject of a FOIA request must be evaluated to determine in each instance whether one or more FOIA exemptions apply.

(3) SBU information is categorized in one or more of the following groups:

- Tax data (e.g. tax returns, returns information, and taxpayer information)
- Law enforcement information (e.g., grand jury, informant, and undercover operations information)
- Proprietary information (e.g., contracts, solicitations, information covered by the Trade Secrets Act, the Procurement Integrity Act, and similar statues)
- Employee Information (e.g., personnel, payroll, and evaluation data)
- Personally Identifiable Information (PII) (i.e., all taxpayer information or any combination of information that can be used to uniquely identify, contact, or locate a person)

Note: The Privacy Act of 1974, 5 U.S.C. § 552a, provides statutory recognition of an individual's right to privacy. For example, the Privacy Act protects information which is retrieved by reference to a name or other personal identifier, such as a social security number or SEID.

(4) All employees who have had access to tax data or privacy information are prohibited from disclosing such information except as authorized by law (and implementing regulations); see IRM 11.3, Disclosure of Official Information (*various chapters*). Employees should safeguard SBU information in order to avoid the loss or the unauthorized disclosure or destruction of files, irrespective of the format in which it is maintained (e.g., paper, electronic, or other media).

(5) Standard practice is to maintain SBU files and documents in locked cabinets or compartments (e.g., desk drawers, overhead bins) during nonworking hours and during periods when the work area is vacant. The records may also be stored in a room with physical access control measures that prevent unauthorized access by the public, visitors, or other persons without a need-to-know.

Examples of acceptable access control measures include, but ar not limited to, a locked room (both key or cipher locks) or a restricted-access work area controlled by a card reader.

a. Employees should store all electronic records containing SBU/PII on the Chief Counsel network.
b. All SBU/PII that is processed, stored, or transmitted by computer equipment (such as laptops and memory storage devices) outside of IRS facilities must be encrypted.

(6) Employees should use measures appropriate to the circumstances to protect SBU information on desks, on workstations or in conference or other work rooms when they are not present during the workday, in order to prevent unauthorized access.

(7) Employees should immediately report allegations or information regarding unauthorized disclosure of tax data or privacy information to their manager for referral to the Treasury Inspector General for Tax Administration (TIGTA) office.

(8) Additional information is available in:

- *CCDM 30.9.1* , Case File Management
- *CCDM 37.1.1* , Written Determinations Under Section 6110
- *CCDM 37.1.2* , Disclosure of Information
- *CCDM 37.2.1* , Privacy Act of 1974
- *CCDM 39.1.2* , Government Ethics Programs
- *IRM 10.5.1*, Privacy Policy
- *IRM 1.4.6*, Managers Security Handbook
- IRM 10.8.1, Information Technology (IT) Security, Policy, and Guidance
- IRM 10.9.1, National Security Information
- IRM 11.3.1, Introduction to Disclosure
- IRM 11.3.12, Classification of Documents
- Document 10281, Safeguarding Taxpayer Records — Renewing our Commitment

30.6.1.2.1
(01-30-2008)
Documents Classified as "Official Use Only"

(1) Within the Office of Chief Counsel, documents may be classified Official Use Only (OUO) by the persons authorized in Delegation Order No. 89, Administrative Control of Documents and Material, as revised (see IRM 1.2.49, Delegations of Authority for Communications, Liaison and Disclosure Activities). This classification is used for documents which may be made available only to authorized personnel.

(2) The overall principle is that the greatest amount of information will be made available to the public whenever possible. The OUO classification will generally be used only for law enforcement matters if publication would hinder the law enforcement process. OUO classification is generally invoked word by word or line by line, so that only the specific words or lines that need to be classified are in fact classified.

(3) The classification of materials as Official Use Only requires the concurrence of the office of the Director, Governmental Liaison and Disclosure, and shall be coordinated by the Deputy Associate Chief Counsel (Legislation and Policy).

(4) For additional guidance on use of the Official Use Only classification, see *IRM 11.3.12* , Designation of Documents.

30.6.1.2.2
(03-29-2006)
Disposition of SBU and OUO Information

(1) All Sensitive But Unclassified (SBU) documents and documents classified ″Official Use Only″ (OUO) must be placed in a designated container for disposal, separate from wastepaper baskets or paper recycling receptacles.

(2) In the Headquarters Office, each Administrative Officer will establish a pick-up point in the office for collection and proper disposal of SBU and OUO information.

(3) In field offices, each Finance and Management (F&M) Office Manager is responsible for establishing procedures for the proper disposal of SBU and OUO information.

30.6.1.2.3
(03-27-2020)
Electronic Mail and Messaging

(1) Electronic mail (email) is provided for official business purposes.

(2) Employees should evaluate the propriety of email as the communication vehicle for particular information or work products. If there is doubt as to whether email is appropriate, employees should check with their manager. Guidance on the use of email may be found in *IRM 1.10.3*, Standards for Using EMail, and in *IRM 10.5.1.6.8*, Privacy and Information Protection, Privacy Policy, Email.

(3) Where appropriate, Enterprise Remote Access Protocol (ERAP) and encryption must be used for email to IRS employees.

(4) Email messages or email attachments to recipients outside the IRS that contain PII or taxpayer information must be encrypted, using an IRS-approved encryption method. If the email is to a taxpayer or taxpayer representative, a Memorandum of Understanding (MOU) in which the taxpayer acknowledges the risks of using email must be executed prior to sending any such email. The MOU form differs depending on the type of encryption used. The procedures for sending encrypted email to recipients outside the IRS and the appropriate MOU forms may be found on the Litigation Technology Page of the Chief Counsel Intranet. Chief Counsel's use of encrypted email in communications with taxpayers or taxpayer representatives in connection with Tax Court litigation, letter rulings or closing agreements is an authorized secure email program under *IRM 10.5.1.6.8.1(2)*.

(5) Routing and review procedures for email are the same as for letters and memoranda. Unless otherwise requested or unless simultaneous review is necessary, work products should be sent to the addressee(s) through customary supervisory/review channels.

(6) ″Broadcast/All User″ email messages should receive pre-authorization in the headquarters office by an Associate Chief Counsel. In field offices, ″All User″ messages should be approved by the Area Counsel; cross-functional messages should be approved by the Managing Counsel or F&M Area Manager. ″All User″ email messages should include the name and title of the authorizing official.

(7) Microsoft Skype and Lync are Microsoft messaging applications that facilitate informal, unofficial communication between employees. Chief Counsel has made an institutional decision to not conduct official business via Skype or

Lync, or other non-email messaging applications, including text messaging. Outlook is not configured to automatically save Skype and Lync communications. If a conversation in Skype, Lync, or any other messaging application rises to the level of official business, the Chief Counsel user must take appropriate measures to preserve the conversation. Documents shared via Skype and Lync retain the status such documents had when originally created, and the appropriate document retention policies and discovery obligations remain applicable to those documents.

(8) Confidentiality requirements for taxpayer returns and return information, as those terms are defined in IRC 6103(b)(1) and (2), are not changed by the use of email or messaging.

(9) Email and other forms of electronic messaging are potentially subject to disclosure under the Freedom of Information Act (FOIA) and the applicable rules of civil or criminal discovery in litigation, to the same extent as paper documents. Communications for which privileges may be available (e.g., attorney-client, attorney work product) apply to email and other forms of electronic messaging as well as to traditional formats.

(10) Record retention and preservation guidelines apply to email and other forms of electronic messaging communications based on their content. Guidelines may be found in *IRM 1.15.6*, Managing Electronic Records, and in the records control schedule for Chief Counsel (see NARA Request for Records Disposition Authority for Chief Counsel Records, DAA-0058-2012-0005 (December 1, 2015) to be incorporated into Document 12990, Records Control Schedules).

30.6.1.2.4
(01-30-2008)
Records Statutes, Records Control Schedules and Disclosure

(1) For assistance with legal questions concerning the application of Federal records statutes or regulations, contact the Associate Chief Counsel (General Legal Services).

(2) The records control schedules for Chief Counsel can be found at:

- Records Control Schedule for the Chief Counsel - page 63 of *Records Control Schedules*
- Records Control Schedule for Internal Revenue Service for Associate Chief Counsel Offices - page 68 of *Records Control Schedules*
- Records Control Schedule for Regional/District Counsel - page 78 of *Records Control Schedules*

(3) Contact the National Records Officer or the local records officer with questions about the existence or identity of general records schedules or record control schedules covering a particular record or records.

(4) For assistance with issues related to accessing or disclosing Service records pursuant to IRC § 6103, FOIA, or the Privacy Act, contact Branches 6 and 7 in the Office of the Associate Chief Counsel (Procedure and Administration).

30.6.1.3
(04-29-2009)
Security of Personnel and Property

(1) The Office of Chief Counsel is committed to providing for the security of its employees and will seek to minimize or eliminate safety hazards and to encourage safe practices. Further information can be found in the following:

- *IRM 10.2.5.5*, Authorized ID Media
- *IRM 10.2.5*, Identification Card
- *IRM 1.14.5*, Occupational Safety and Health Program

(2) The Office of Chief Counsel will follow the guidelines established by IRS, Department of the Treasury, GSA, and the Department of Homeland Security.

(3) Employees should ensure that information, documents and property entrusted to them are secured. Those who are in private offices have the responsibility of locking doors when leaving their work areas. Employees should keep personal valuables in their possession.

(4) Employees are responsible for preventing unauthorized entry into areas where government information, documents and property are located.

(5) At the close of business, managers should ensure that doors leading into areas under their control and supervision are locked.

(6) Employees should immediately report burglary, robbery, or theft of government or personal property to their manager and to the servicing Security Office. All thefts, no matter how small, should be reported.

30.6.1.3.1
(03-29-2006)
Identification Media

(1) Employees are responsible for the security of pocket commissions, ID cards (badges) and other types of identification media issued to them. Identification media should be in the possession of employees and should never be left unattended in briefcases, unlocked desk drawers, vehicles, etc. When not in use they should be stored in a locked container or left with a manager.

(2) Employees will display ID cards at all times while in IRS facilities.

(3) Employees must immediately report the loss, theft or destruction of identification media through their manager to the servicing Security office. The report should explain the circumstances and describe the recovery attempts made.

(4) The recovery of any type of identification media should be reported through channels to the issuing Security office.

30.6.1.3.2
(04-29-2009)
Protection Standards

(1) The policy of the Office of Chief Counsel is to provide reasonable protection commensurate with the nature and value of the information or property involved. Protective measures will vary by location, function and facility.

(2) In general, access to space, property and the information contained therein will be restricted to those with a need for access.

(3) For Counsel-specific guidelines, see *CCDM 30.5.1*, Space, Property, Procurement, and Telecommunications.

(4) For IRS access and protection standards, see:

- *IRM 10.2.14* , Methods of Providing Protection
- *IRM 10.2.15* , Minimum Protection Standards

(5) Where feasible, reception areas will be provided. Conference rooms and other areas expected to be used by visitors will be placed near entrances and away from secured or restricted areas.

30.6.1.3.3
(03-29-2006)
Access Control

(1) Employees will be required to sign a receipt for door keys, building keys and electronic access cards issued to them. Under no circumstances should keys be duplicated by employees.

(2) Employees are responsible for reporting the loss of keys or access cards to the Administrative Officer (employees located in Headquarters offices) or F&M Office Manager (field offices). The Administrative Officer or Office Manager is responsible for reporting key reassignments and losses to the local IRS Security office.

(3) Codes for combination locks and key pads should be changed:

- At least once every six months
- When anyone with the current combination leaves or is terminated
- When an attempt to compromise the combination is made

(4) Keyed locks should be changed periodically as the budget permits.

(5) Electronic access cards, door keys and building keys must be returned when employees resign, retire, are reassigned to another office, or are terminated.

30.6.1.3.4
(03-29-2006)
Mail Handling

(1) In response to various incidents in the US Postal Service (USPS) system, all Counsel mail, regardless of the source or method of delivery (e.g., overnight delivery services), will be opened prior to delivery. The only exceptions are bulk mail and mail that has been irradiated by USPS. Deliveries should be made to the area specified by the Agency-Wide Shared Services (AWSS) representative for the building.

(2) Employees opening mail should take appropriate precautions; protective supplies will be provided by IRS or Counsel.

(3) Office Managers and headquarters Administrative Officers should prominently post guidelines for processing mail and packages in the mail area, including phone numbers for appropriate Security personnel. They may obtain further information from their servicing Security office.

(4) Employees should be alert to suspicious packages which may:

- Appear unusual
- Carry excessive postage
- Display restrictive endorsements such as “Personal” or “Confidential”
- Contain misspelled or misidentified names, titles, addresses or organizations
- Be unexpected mail from a foreign country

(5) If a suspicious package is discovered, employees should not handle the package or remove any items from the area. They should leave the area, gently close the door, and contact their manager. If a biochemical substance is suspected, the employee should immediately contact the Security office and follow their direction.

30.6.1.3.4.1
(03-29-2006)
Mail Delays

(1) The current USPS procedures in response to anthrax threats may cause delays in sending mail to the Tax Court, Department of Justice, or other Federal offices in the Washington, D.C. area.

(2) Employees should be aware of possible delays and should consider whether overnight delivery or some form of electronic transmission (fax or email) is a suitable alternative if the material is truly time sensitive.

(3) Procedures for addressing legal issues resulting from delays in mail destined for the Tax Court are covered in more detail in CCDM Part 35.