JRIC - Safeguarding Sensitive but Unclassified Information

For Official Use Only (FOUO)

FOUO is the marking used by DHS to identify Sensitive but Unclassified information within the DHS community, the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of federal programs, or other operations essential to the national interest and that is not otherwise covered by a statute or regulation.

Other government agencies and international organizations frequently use different terms to identify sensitive information, such as "Limited Official Use (LOU)," "Official Use Only (OUO)," and in some instances "Law Enforcement Sensitive (LES)." In most instances the safeguarding requirements for this type of information are equivalent to FOUO.

However, other agencies and international organizations may have additional requirements concerning the safeguarding of their sensitive information. When available, follow the safeguarding guidance provided by the other agency or organization. Should no guidance be available the information will be safeguarded in accordance with FOUO guidance provided in this booklet.

It is not permitted to mark information as FOUO to conceal government negligence, ineptitude, or other disreputable circumstances embarrassing to a government agency.

Marking

Information determined to be FOUO will be sufficiently marked so that persons granted access to it are aware of its sensitivity and protection requirements. At a minimum, it is marked on the bottom of each page "FOR OFFICIAL USE ONLY." Materials containing specific types of FOUO information can be further marked with an applicable caveat, e.g. "LAW ENFORCEMENT SENSITIVE," in order to alert the reader of the type of information conveyed. Additional access and dissemination restrictions may also be cited as the situation warrants.

Markings typically associated with classified information such as originator information, downgrading instructions, and date/event markings are not required on FOUO documents.

Access and Dissemination

A security clearance is not needed for access to FOUO information. Access to FOUO information is based on a "need-to-know" as determined by the holder of the information. Where there is uncertainty as to a person's need-to-know, the holder should request dissemination instructions from the JRIC.

FOUO information may be shared with other agencies, federal, state, private sector, or local government and law enforcement officials, provided a need-to-know has been established and the information is shared in the furtherance of an official government activity, to include homeland defense, and no dissemination restrictions have been cited by the originator.

When discussing FOUO information over a telephone, use of the STU-III or STE is encouraged, but not required.

FOUO information may be transmitted via non-secure fax machine, although the use of a secure fax is encouraged. Where a non-secure fax machine is used ensure that a recipient is present at the time of the fax and that the materials faxed will not be left unattended or subject to unauthorized disclosure.

FOUO information may be transmitted over official email channels. However, it shall not be sent to personal email accounts. For added security when transmitting FOUO information by email, password protected attachments may be used with the password transmitted or otherwise communicated separately.

Do not enter or post any FOUO information on any public website.

FOUO information may be mailed by regular US Postal Service first class mail or any commercial mailing service.

Storage

When unattended, FOUO information shall be stored in a locked filing cabinet, locked desk drawer, a locked overhead storage compartment such as systems furniture credenza, or a similar locked compartment. Information can also be stored in a room or area that has sufficient physical access control measures to afford adequate protection and prevent unauthorized access by members of the public, visitors, or other persons without the need-to-know, such as a locked room or an area where access is controlled by a guard, cipher lock, or card reader.

Destruction

- Hard copy FOUO materials will be destroyed by shredding, burning, pulping, or pulverizing, sufficient to assure destruction beyond recognition and reconstruction.

- After destruction, materials may be disposed of with normal waste.

- Electronic storage media shall be sanitized appropriately by overwriting or degaussing.

- Paper products or electronic media containing FOUO information will not be disposed of in regular trash or recycling receptacles unless the materials have been destroyed as specified above.

Incident Reporting

- Compromise, suspected compromise and suspicious or inappropriate requests for FOUO information shall be reported to the JRIC or the originator of the information.

- Additional guidance or assistance can be obtained by contacting DHS or FBI security officers.