CRITICAL INFRASTRUCTURE AND KEY RESOURCES SECTOR MEMBER GUIDE

HANDLING AND DISSEMINATING SENSITIVE BUT UNCLASSIFIED INFORMATION

This document provides guidance to the owners and operators of the 18 Critical Infrastructure and Key Resources (CIKR) Sectors on how to properly identify, handle, and disseminate information that may be considered Sensitive But Unclassified Information (SBU) by the Department of Homeland Security (DHS). Specifically, this document defines and outlines the sector member responsibilities, risks, and consequences of working with "For Official Use Only" (FOUO) information generated or disseminated by DHS. This paper does not include guidelines on handling sensitive information from other Federal agencies, classified information, or open source information. This guidance is applicable to all members of the 18 CIKR Sectors, their contractors and consultants, and others to whom access to DHS FOUO information is granted.

While within DHS, the term FOUO is used to identify information that has been categorized as SBU, sensitive information of importance to the CIKR Sectors can fall into several other distinct categories that are independently governed by statute and/or regulation and beyond the categorical designation of FOUO. Should the Federal Government determine that the information meets the standards for these other categories, their specific guidance takes precedence for the purposes of marking, handling, and safeguarding the information.

DEFINITION - FOR OFFICIAL USE ONLY

A document's sensitivity determines the availability and accessibility of content and affects how content is disseminated, shared, and protected. As there is currently no government-wide standard for designating, handling, and disseminating sensitive information that is not otherwise governed by statute or regulation, Federal agencies have chosen to adopt individual standards of their own. DHS has chosen FOUO as the Department's designation for SBU type information and a corresponding set of standards for its designation, handling, and dissemination.

Within DHS, FOUO identifies unclassified information of a sensitive nature – not otherwise categorized by statute or regulation – the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national interest. FOUO is not to be considered classified information.

However, recognizing the inconsistency in the designation, handling, and dissemination of SBU type information among the various Federal agencies, a May 2008 Presidential Memorandum directed Federal agencies to adopt "Controlled Unclassified Information" as the "*...single, categorical designation henceforth throughout the executive branch for all information within the scope of that definition, which includes most information heretofore referred to as 'Sensitive But Unclassified' (SBU) in the Information Sharing Environment...*" Efforts to develop policies and procedures for implementation of the President's direction are on-going with implementation anticipated for calendar year 2011. Until such time as these policies and procedures are appropriately promulgated, followed by an intense training regimen, guidelines for FOUO remain in effect.

The following types of information are treated as FOUO information:

- Information that may be exempt from FOIA disclosure;
- Information that is exempt from disclosure under the Privacy Act;
- International and domestic information protected by statute, treaty, or other agreements;
- Information that could be sold for profit;
- Information that could result in physical risk to personnel;
- DHS information technology (IT) internal systems data;
- Government systems security data revealing the security posture of the system, including threat assessments, system security plans, contingency plans, risk management plans, Business Impact Analysis studies, and Certification and Accreditation documentation;
- Reviews or reports illustrating or disclosing facility infrastructure or security vulnerabilities;
- Information that could constitute an indicator of U.S. government intentions, capabilities, operations, or activities or otherwise threaten operations security; and
- Developing or current technology, the release of which could hinder the objectives of DHS, compromise a technological advantage or countermeasure, cause a denial of service, or provide an adversary with sufficient information to clone, counterfeit, or circumvent a process or system.

CIKR MEMBER RESPONSIBILITIES

The holder of FOUO information generated or disseminated by DHS is responsible for knowing and understanding their responsibilities for the proper handling and dissemination of the information. The following basic guidelines pertain to the responsibilities of the recipient of the information:

In general:

- As of 2008, there were more than 100 markings and handling processes for SBU type information across the Federal Government.[1] The guidance provided by the originating agency should be followed for handling this information. If no guidance is provided, the information should be safeguarded consistent with DHS's FOUO guidance.
- If no markings are present on the document and the holder suspects that the information is sensitive in nature, it should be safeguarded consistent with DHS's FOUO guidance.

Report suspicious or inappropriate requests for information to the National Infrastructure Coordinating Center (202-282-9201)

Dissemination, Access, and Handling:

- The holder of the information should ensure that FOUO information is only disseminated to recipients who require access to the information in order to perform or assist a lawful governmental function. Where there is uncertainty about a recipient's appropriate level of access, the holder of the information should request instructions from the information's originator or the applicable DHS program office.
- Private sector entities are permitted to share DHS FOUO information provided there are no identified restrictions on further dissemination and the intended recipient(s) have a need for access to the information in support of the protection of CIKR assets and resources.
- When transmitting in any manner, take precautions to prevent unauthorized individuals from overhearing the conversation, observing the materials, or otherwise obtaining the information.
- A security clearance is not required to access FOUO information.
- FOUO information may not be posted on any Internet website or sent to personal email accounts.
- FOUO information may be posted on the DHS intranet or other government controlled or sponsored networks, such as the Homeland Security Information Network (HSIN).

- *FOUO materials should be stored in a locked file cabinet, drawer, or office, and separate from materials labeled with other handling designations or classifications.*
- *FOUO materials should be destroyed, such as by shredding, and not disposed of in regular trash or recycling bins unless first destroyed.*

CIKR MEMBER RISKS & CONSEQUENCES

Risks and consequences for non-government handling of SBU vary from those of Federal Government employees. The following critical issues should be considered by the private sector when handling FOUO information generated by DHS. Private sector recipients have no explicit legal liability for disclosing FOUO information, whether accidentally or otherwise. However, failure to safeguard the information could lead to consequences such as:

- Losing access to future information from government sources
- Hesitancy by DHS or other Federal agencies to share information
- Hesitancy by other private sector participants to share information
- Compromise of sensitive operations or activities
- Private sector entities who are also government contractors may face contractual penalties (which could include losing contracts) if they do not handle the information in accordance with applicable guidelines.
- Information designated as FOUO is not automatically protected from disclosure under FOIA. Information requested by the public under a FOIA request will be reviewed on a case-by-case basis.
- There are risks of confusion and administrative burden for those sectors whose Sector Specific Agency (SSA) is not DHS and uses protection mechanisms other than FOUO, as defined by DHS.

[1] http://www.dhs.gov/xlibrary/assets/privacy/privacy_dpiac_june112008_afternoon_minutes.pdf at 39

OTHER TYPES OF HANDLING DESIGNATIONS FOR SENSITIVE INFORMATION

Within the purview of DHS, Sensitive But Unclassified Information of importance to the CIKR sectors can further fall into several distinct subcategories. Should the Federal Government determine that the information meets the standards for these categories, their specific guidance takes precedence for the purposes of marking, handling, and safeguarding the information. Information marked in accordance with such guidance need not be additionally marked FOUO.

Protected Critical Infrastructure Information (PCII)

Protected Critical Infrastructure Information (PCII) ensures that voluntarily submitted critical infrastructure information will be exempt from public disclosure, will not be used for regulatory purposes, and will be properly safeguarded. Information under PCII includes that which is not customarily in the public domain and related to the security of critical infrastructure or protected systems. More information can be found at the following website:
http://www.dhs.gov/xinfoshare/programs/editorial_0404.shtm

Sensitive Security Information (SSI)

Sensitive Security Information (SSI) is a designation used by the Transportation Security Administration for sensitive transportation-sector information requiring protection against disclosure. This includes information obtained or developed in carrying out certain security or research and development activities to the extent that it has been determined that disclosure of the information would be an unwarranted invasion of personal privacy; reveal a trade secret or privileged or confidential commercial or financial information; or be detrimental to the safety of passengers in transportation.[1]

Chemical-terrorism Vulnerability Information (CVI)

Chemical-terrorism Vulnerability Information (CVI) is the information protection regime to protect from inappropriate public disclosure information relating to vulnerability and security exchanged between DHS and facilities that produce or handle potentially dangerous quantities of chemicals. This includes information developed pursuant to the Chemical Facility Anti-Terrorism Standards (CFATS), Security Vulnerability Assessments, Site Security Plans, and Alternative Security Programs. More information can be found at the following website:
http://www.dhs.gov/xprevprot/programs/gc_1181835547413.shtm

[1] Unlike PCII and CVI, there is no comprehensive government website for SSI but information about SSI can be found in various university papers and GAO Reports.