DISTRICT OF COLUMBIA
FIRE AND EMERGENCY MEDICAL SERVICES DEPARTMENT

_____

| **Bulletin 12** | **June 2010** |

Handling Sensitive, but Unclassified Information Policy

1.   PURPOSE

1.1   This policy sets forth mandatory requirements regarding the identification, access, dissemination, storage, and destruction of documents, produced by D.C. Fire & EMS Department or any other Federal, state, tribal, or local government agency or private sector entity, that are designated as Sensitive but Unclassified.

2.   SCOPE

2.1   This procedure applies to all uniformed members and civilian employees of D.C. Fire & EMS Department.

3.   HANDLING SENSITIVE BUT UNCLASSIFIED INFORMATION POLICY

3.1   For Official Use Only (FOUO) Materials

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

3.1.2   "Controlled Unclassified Information" (CUI) is used by the executive branch to designate information that was previously shared under "Sensitive but Unclassified (SBU)" label.

3.1.3   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.

3.1.4   LES designation is most appropriately applied to information related to an ongoing criminal case. This designation does not limit information sharing with Fire and EMS personnel with a need to know that information.

3.1.5   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 the FOUO guidance provided here.

3.2   Marking

3.2.1   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.

3.3   Access and Dissemination

3.3.1   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 their next-level supervisor or the originating activity.

3.3.2   FOUO information may be shared with other agencies, Federal, state, tribal, 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 governmental activity, to include homeland defense, and no dissemination restrictions have been cited by the originator.

3.3.3   FOUO information may be transmitted via non-secure fax machine within DC Fire & EMS Department. 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.

3.3.4   FOUO information may be transmitted over DC Fire & EMS Department email channels. However, it shall NOT be sent to personal email accounts. Do NOT enter or post any FOUO information on any public website.

3.4 Storage

    3.4.1 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.

3.5 Destruction

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

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

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

    3.5.4 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.

3.6 Incident Reporting

    3.6.1 Compromise, suspected compromise and suspicious or inappropriate requests for FOUO information shall be reported immediately to the on-duty Special Operations Battalion Fire Chief.

    3.6.2 Additional guidance or assistance can be obtained by contacting the Battalion Fire Chief - Homeland Security.

4. Monday Report – Intelligence Briefing – U/FOUO

4.1 The Homeland Security Office will attempt to distribute a weekly intelligence briefing as the intelligence / information warrants.

4.2   Format

    4.2.1   A single PowerPoint program format is used, with two versions:
- **Standard** – BLUE version will be used to disseminate general information out to the entire Department.
- **Critical** – RED version will be used to disseminate time sensitive critical out to the entire Department
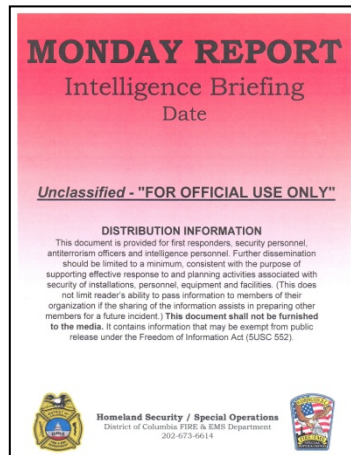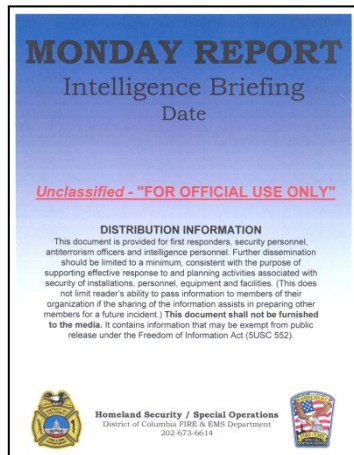
    4.2.2   Both versions are clearly labeled "*Unclassified* **– FOR OFFICIAL USE ONLY**", and have a cover sheet with distribution information.

4.3   Development

    4.3.1   The Homeland Security Office compiles events and/or information that meet the following criteria:
- Timely
- Important /relevant to the Department
- Broad based information

    4.3.2   If the information to be used has already been developed by another source, it is used in that format, giving credit to the source.

    4.3.3   Topics are developed from several sources:
- Intelligence analysis reports
- Open source reporting
- Standing intelligence requests from WRTAC
- DHS reports

    4.3.4   The 'DRAFT' document is distributed to the following to address concerns and proof for corrections:

- Assistant Fire Chief – Operations
- Deputy Fire Chief – Special Operations
- Battalion Fire Chief – Homeland Security

4.4   Access and Dissemination for a **Standard** (BLUE) Issue

    4.4.1   Once all concerns and corrections have been addressed for a **Standard** (BLUE) issue, the document is embedded into a standardized D.C. Fire & EMS Department email format that is sent out to all Special Operations Battalion Fire Chiefs.

    4.4.2   The Special Operations Battalion Fire Chiefs may then forward the email, along with any additional comments, to the company officers within the Special Operations Battalion and review with the companies as appropriate.

    4.4.3   Once all concerns and corrections have been addressed for a **Standard** (BLUE) issue, the document is embedded into a standardized D.C. Fire & EMS Department email format that is sent out to all Deputy Fire Chiefs.

    4.4.4   The Deputy Fire Chief may then forward the email, along with any additional comments, to their respective Battalion Fire Chiefs. The Battalion Fire Chiefs will review with the members / companies within their respective Divisions / Battalions.

    4.4.5   Once all concerns and corrections have been addressed for a **Standard** (BLUE) issue, it is converted into a single PDF format that is **locked** to prevent copying and printing and it is posted in the 'FireWatch' folder on the LAN that can be accessed by all D.C. Fire & EMS Department members for review.

4.5   Access and Dissemination for a **Critical** (RED) Issue

    4.5.1   When there has been a determination by either the Assistant Fire Chief – Operations or the Deputy Fire Chief – Special Operation that the intelligence / information is critical or time sensitive a **Critical** (RED) Issue will be developed.

    4.5.2   Once all concerns and corrections have been addressed for a **Critical** (RED) issue, it is converted into a single PDF format that is **locked** to prevent copying and printing and it is posted in the 'FireWatch' folder on the LAN that can be accessed by all D.C. Fire & EMS Department members for review.
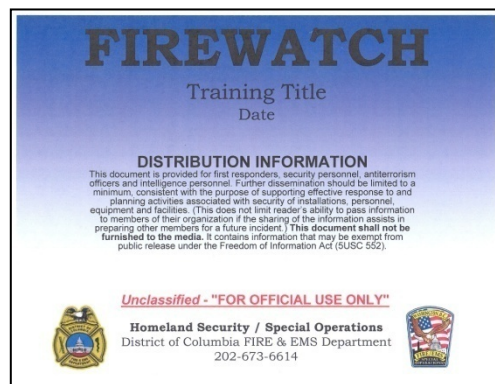
4.5.3   Then through the Department, a 'stand-down' or like event is used to inform the entire Department to review the document will be issued.

5.   FireWatch – Training Program

5.1   The Homeland Security Office will attempt to distribute a monthly training document as the intelligence / information warrants.

5.2   Format

5.2.1   A single PowerPoint program format is used:

5.2.2   The cover sheet is clearly labeled "*Unclassified* **– FOR OFFICIAL USE ONLY**", and contains distribution information.

5.3   Development

5.3.1   The Homeland Security Office will compile events and/or information that meet the following criteria:
   - Item specific topics
   - Short, 12-15 slides
   - Covering the topic and related Department policies
   - Broad based information

5.3.2   Topics are developed from several sources:
   - Department Manuals and SOGs
   - Topic recommendations from Battalion Fire Chiefs
   - Intelligence analysis reports
   - Open source reporting
   - DHS reports

5.3.3   The DRAFT document is distributed to the following:
- Assistant Fire Chief – Operations
- Deputy Fire Chief – Special Operations
- Battalion Fire Chief – Homeland Security
- Special Operations Battalion Fire Chiefs
- Subject matter experts as needed

5.4   Access and Dissemination for a FireWatch – Training Program Issue

5.4.1   Once all concerns and corrections have been addressed for a FireWatch – Training Program issue, it is converted into a single PDF format that is **locked** to prevent copying and printing and it is posted in the 'FireWatch' folder on the LAN that can be accessed by all D.C. Fire & EMS Department members for review.