Office of the Secretary
Office of State and Local Government Coordination & Preparedness
Washington, DC 20531

Homeland Security

ODP Information Bulletin
No. 188, August 19, 2005

TO: All State Administrative Agency Heads
All State Administrative Agency Points of Contact

FROM: Matt A. Mayer
Acting Executive Director

SUBJECT: FY 2005 Transit Security Grant Program Requirements

The Office of State and Local Government Coordination and Preparedness (SLGCP) has established a policy for the handling and use of Sensitive Security Information (SSI) submitted by grantees as required by the FY 2005 Transit Security Grant Program (TSGP). This information is intended to provide additional information regarding this policy.

Purpose and Scope

The purpose is to establish a defined policy regarding the handling, use, and access to information that is determined to be Sensitive Security Information (SSI) originating within SLGCP and submitted to SLGCP as a requirement of the grant process. This policy addresses, specifically, the Regional Transit Security Strategy (RTSS), Security and Emergency Preparedness Plans (SEPP), and Risk Assessments submitted to meet the requirements of the FY 2005 TSGP.

This policy applies to all SLGCP headquarters, components, organizational elements, detailees, contractors, consultants, and others to whom access to information covered by this policy is granted.

Access

Access to information designated as SSI is limited to those with a need to know. Need to know is defined as: “a prospective recipient requires access to specific information in order to perform or assist in a lawful and authorized governmental function, i.e. access is required for the performance of official duties.” Information designated as SSI is also exempt from disclosure under the provisions of the Freedom of Information Act, 5 § U.S.C. 552 (FOIA).

AUTHENTICATED U.S. GOVERNMENT INFORMATION GPO

Additional Information

For your convenience, a complete document containing the policy is attached. This document is also available on the ODP Secure Portal at: https://odp.esportals.com/.

For specific information concerning eligibility and grant guidelines, please refer to the TSGP application kit at http://www.ojp.usdoj.gov/odp/docs/fy2005tsgp.pdf. Questions related to this grant program may be directed to tsgp@dhs.gov or to the SLGCP Centralized Scheduling and Information Desk 1-800-368-6498. Frequently asked questions regarding the TSGP will be addressed in bi-weekly conference calls every other Wednesday from 1:30-2:30 p.m. EST, beginning April 20th.

Attachment

MEMORANDUM TO: All SLGCP Employees

FROM: Matt A. Mayer /s/
Acting Executive Director

SUBJECT: **SLGCP Policy Memorandum No. 05-06: Sensitive Security Information (SSI)**

DATE: **August 9, 2005**

SLGCP Policy Statement

Sensitive Security Information (SSI), as defined in 49 C.F.R. § 15, is a specific category of information that requires protection against disclosure. Within SLGCP, the following types of information will be treated as SSI:

- Any security contingency plan or information and any comments, instructions, or implementing guidance pertaining thereto under the rules listed in 49 U.S.C. § 1520.5(a) (1) through (6).
- Information concerning threats against transportation.
- Information regarding critical aviation, surface transportation, or maritime infrastructure assets.
- Any draft, proposed, or recommended change to the information and records identified in this section.
- Any other information, the disclosure of which is prohibited under the criteria of 49 U.S.C. § 40119.

For purposes of this policy, SSI includes information originating from within SLGCP as well as other sensitive but unclassified information received by SLGCP from other government and non-government activities. Specifically, this includes the Regional Transit Security Strategies, Security and Emergency Preparedness Plans, and Risk Assessments submitted as part of the Transit Security Grant Program (TSGP). At this time, information that may need to be raised to a classified level can be reviewed against the National Exercise Program Security Classification Guide to establish classification.

It is SLGCP policy that information will not be designated as SSI unless necessary. In addition, information designated SSI is exempt from disclosure under the provisions of the Freedom of Information Act.

Any SLGCP employee, detailee, or contractor can designate information falling in the categories identified on page 1 as SSI. Officials occupying supervisory or managerial positions are authorized to designate other information, not listed above and originating under their jurisdiction, as SSI. Information designated as SSI will retain its designation until determined

otherwise by the originator or a supervisory or management official having program responsibility over the originator and/or information.

SLGCP employees, detailees, contractors, consultants, and others to whom access is granted are expected to:

- Be aware of and comply with the safeguarding requirements for SSI as outlined in this policy.
- Participate in training sessions presented to communicate the requirements for safeguarding SSI and other sensitive but unclassified information as outlined in DHS Management Directive 11042.1.
- Be aware that divulging information without proper authority could result in administrative or disciplinary action.

Supervisors and managers are expected to:

- Ensure that an adequate level of education and awareness is established and maintained for employees.
- Take appropriate corrective actions, to include administrative or disciplinary action as appropriate, when violations occur.

Procedures for Implementation

- Contractors and consultants must execute a DHS form 11000-6, Sensitive but Unclassified Information Non-Disclosure Agreement (NDA), as a condition of access to SSI. In addition, other individuals not assigned to or contractually obligated to DHS, but to whom access to information will be granted, may be requested to execute an NDA as determined by the applicable program manager. Execution of the NDA is effective upon publication of this policy and not applied retroactively.

- When creating a record containing SSI, you must include a protective marking and limited distribution statement that clearly identifies the information as SSI and specifies the distribution limitation required. If you receive a record containing SSI that is not correctly marked, you must apply the appropriate marking and inform the sender of its omission.

- Specifically, the **protective marking** must:

  - ✓ consist of the words **"SENSITIVE SECURITY INFORMATION";**
  - ✓ be written or stamped in plain style bold type, such as Times New Roman and a font size of 16, or an equivalent style and font size; and
  - ✓ be applied to all documents that contain SSI.

- The following **distribution limitation statement** must be applied to all documents that contain SSI:

  "<u>WARNING</u>: This document contains Sensitive Security Information that is controlled under 49 CFR Part 15. No part of this document may be released to persons without a need to know, as defined in 49 CFR Part 15, except with the written permission of DHS, Washington, DC. Unauthorized release may result in civil penalty or other action. For U.S. Government agencies, public release is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520."

  This distribution limitation statement should be written or stamped in plain style bold type (e.g., Times New Roman) with a font size of 8, or an equivalent style and font size.

- The following marking requirements apply to all records containing SSI that are created after the date of this policy memorandum, and to all existing records containing SSI, prior to release:

  - ✓ **<u>Documents:</u>** Apply the **protective marking** at the top of the outside of any front cover (including a binder or folder), on the top of any title page, on the top of the first page and each subsequent page, and on the top of the outside of any back cover (including a binder or folder). Apply the **distribution limitation** statement at the bottom of the outside of any front cover (including a binder or folder), on the bottom of any title page, on the bottom of the first page and each subsequent page, and on the bottom of the outside of any back cover (including a binder or folder).

  - ✓ **<u>Electronic and Magnetic Media</u>:** SSI contained on electronic and magnetic media must have protective markings and the distribution limitation statement applied at the beginning and end of the electronic and magnetic text. The protective marking and distribution limitation statement must be displayed so that both are fully visible on the screen or monitor when the text is viewed. The protective marking and distribution limitation statement must also be applied to each side of the disk and the disk sleeve/jacket, on the non-optical side of the CD-ROM, and on both sides of the CD-ROM case. If the electronic/magnetic text has a soundtrack, audible warnings that describe the protective marking and distribution limitation statement must, if possible, be included in the introduction and at the end of the text.

  - ✓ **<u>Videotape Recordings</u>**: Include conspicuous visual protective markings and distribution limitation statements at both the beginning and the end of the recording, if practicable. In addition, apply protective markings and the distribution limitation statement on the front and back and on each side of the video case and storage containers.

  - ✓ **<u>Charts, Maps, and Drawings</u>**: Affix the **protective marking** and **limited distribution statement** in a manner that it is plainly visible.

- ✓ **Motion Picture Films and Video Recordings**: Apply the **protective marking** and **distribution limitation statement** at the beginning and end of each reel or video recording in such a manner that it is fully visible on the screen or monitor.

- ✓ **Motion Picture Reels:** Apply **protective markings** and **distribution limitation statements** to motion picture reels that are kept in film cans or other containers. Apply them to each side of each reel and to all sides of each can or other storage container. In addition to reproducing the protective marking and distribution limitation statement on the beginning and end portions of the film, if the motion picture film has a soundtrack, if practicable, include audible warnings that describe the protective marking and distribution limitation statement in the introduction and at the end of the film.

- ✓ **Transmittal Documents**: Mark those documents that are used to transmit SSI but do not contain SSI with the distribution limitation statement. In addition, affix the following statement to the front page of the transmittal document:

  "The protective marking SENSITIVE SECURITY INFORMATION and/or the distribution limitation statement on this document are canceled when the attachments containing SSI are removed."

- SLGCP employees and contractor employees must safeguard information and records containing SSI from disclosure to unauthorized personnel at all times. When not in an individual's direct physical control, safeguard and protect the information so that it is not physically or visually accessible to persons who do not have a need to know (e.g., secure SSI in a locked container, office, or other restricted access area). When using a locked container, use container keys or a combination lock to restrict access to the container to only those with a need to know.

- Except as provided below, the authority to release SSI to persons who do not have a need to know is limited to the original designation authority and any other individual formally designated to act in that capacity.

- Information designated as SSI under 49 C.F.R. Part 1520 qualifies for exemption from disclosure under the FOIA based on exemption 3, 5 U.S.C. 552(b)(3)(a). FOIA requests for SSI are processed by SLGCP. Any decision to release SSI must have the concurrence of the Secretary. Requests for information that are addressed to regulated parties, such as under State and local freedom of information or open records acts, should be referred to the SLGCP Executive Director. SLGCP works with affected entities to determine what records or portions of records should remain undisclosed and what may be released.

- If a record contains information that may not be disclosed under 49 C.F.R. Part 15, but also contains information that may be disclosed, in response to a FOIA request, the record may be released if the information is not otherwise exempt from disclosure under FOIA and if it is practical to redact the SSI from the record. If it is not practical to do so, withhold the entire record from public disclosure.

- Prior to a contractor gaining access to SSI, the contractor must meet the processing requirements established by SLGCP. (These requirements are being developed and will

be issued at a later date. In the interim, contractors will be bound by non-disclosure agreements and any other limitations in their contracts.)

- Contractors must provide prior notification in writing, through the Contracting Officer, to the originator of the SSI when the contractor needs to make copies of SSI. This written notification must contain the following minimum information:

  - ✓ positive identification of SSI (title, document numbers as applicable, etc.);
  - ✓ purpose for making copies;
  - ✓ quantity of copies; and
  - ✓ dissemination of copies (the contractor must verify and ensure that all recipients are authorized to receive SSI.).

- Release of SSI is permitted to those with a need to know as established by regulation or authorized by the Executive Director, SLGCP, including:

  - ✓ Federal, state, and municipal government officials/employees and regulated parties.
  - ✓ local law enforcement officials and federal intelligence agencies.

  Refer any other request for SSI to the SLGCP Executive Director.

- SLGCP employees and contractors with knowledge of an **inadvertent release** of SSI must immediately notify the originating authority.

- Transmitting SSI information involves transferring the SSI information from one location to another either by physical relocation or electronic transmission. SLGCP employees and contractors must package and transmit SSI information via physical relocation as follows:

  - ✓ When assembling a package containing SSI for transmission, ensure that all SSI has the appropriate protective markings and distribution limitation statements. Use strong and durable envelopes or containers to provide physical protection during transit and to prevent items from breaking out of the containers or envelopes.

  - ✓ When transmitting by **mail**, use U.S. Postal Service (first class mail or regular parcel post) or other delivery services (Federal Express, UPS, etc). Wrap SSI information in opaque envelopes, wrappings, or cartons. Address the package with an attention line containing the name and office of the recipient to help ensure that the SSI material is received and opened only by authorized personnel.

  - ✓ When sending by **interoffice mail**, seal the envelope in a manner that prevents inadvertent visual disclosure.

  - ✓ When **hand carrying** within or between buildings, protect SSI (by a cover sheet, protective folder, distribution pouch, etc.) to prevent inadvertent visual disclosure.

- SLGCP employees and contractors must transmit SSI information via electronic transmissions (over telecommunications circuits) as follows:

- ✓ When transmitting by **e-mail**, send the SSI in a **password-protected** attachment.

- ✓ **Internet/Intranet postings** of SSI are **not** authorized except for postings on secure sites as specifically authorized by the Executive Director, SLGCP.

- ✓ When transmitting via **facsimile** use the following controls: (1) Confirm that the facsimile number of the recipient is current and valid; (2) If the recipient has a facsimile machine in a controlled area where unauthorized persons cannot intercept the SSI facsimile, send the SSI facsimile without requiring that the recipient be there to receive it promptly. Otherwise, ensure that an authorized recipient is available at the receiving location to promptly retrieve the SSI. (3) Use a cover sheet that clearly identifies the sender's name and telephone number and contains a warning that if the message is received by other than the intended recipient, the individual receiving the message must immediately notify the sender for disposition instructions.

- ✓ When transmitting by **telephone,** ensure that the person receiving the SSI is an authorized recipient. Avoid using cellular and cordless telephones, which transmit the conversation to a base unit, as the risk of interception and monitoring of conversations is greater when using these devices. Refrain from use of these devices unless circumstances are exigent, or the transmissions are encoded or otherwise protected.

- When copies of records containing SSI are no longer needed, they must be promptly and completely destroyed so that the recovery of the sensitive information is difficult, if not impossible. Prior to destruction of SSI, please contact the SLGCP Security Officer for advice on proper destruction.

- Material containing SSI must be destroyed by one of the following methods, listed in order of preference:

  - ✓ Any means approved for the destruction of national security classified material as specified in applicable orders regarding the destruction of national security classified material. The approved means include: burning, pulping, crosscut shredding, melting, chemical decomposition, and mutilation.

  - ✓ Shredding or tearing SSI into small pieces and assimilating it with other waste material. When destroying SSI by hand, cut or tear it into pieces measuring not more than 1/2 inch on a side, and mixed with other wastepaper material in the process.

Related DHS Policies

- DHS Management Directive 11042.1, Safeguarding Sensitive but Unclassified (For Official Use Only) Information

For Further Information Contact

Alan Fisher

Senior Attorney Advisor
202-786-9449

Judy Petsch
SLGCP Security Officer (Contractor)
202-786-9585