STATEWIDE TERRORISM & INTELLIGENCE CENTER
WORK UNIT DIRECTIVE
STIC-018, SECURITY CLASSIFICATIONS OF INFORMATION AND ANALYTICAL PRODUCTS

I. POLICY

The Statewide Terrorism & Intelligence Center (STIC) is a 24 hour/7 day a week call center which provides immediate intelligence information to local, state, and federal law enforcement agencies on suspects of terrorism and major crimes incidents. STIC will establish an information security policy that complies with guidelines established by the U.S. Department of Justice as outlined in "Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era", Washington, D.C., 2006.

II. DEFINITIONS

II.A. Access: The ability or opportunity to gain knowledge of information.

II.B. Confidential: (Highest level unclassified but sensitive information) The term used within STIC to identify unclassified information of a sensitive nature that is meant to have a limited dissemination scope. The term "CONFIDENTIAL" shall not be confused with the federal government's definition of "Confidential" as the lowest level of classified information. Confidential information should not be disseminated outside the ISP, STIC, or others to whom access is granted. Confidential information includes information relating to STIC or ISP operational security, personnel, policy decisions, and on-going analytical products not yet meant to be disseminated outside of STIC or the ISP. (examples: STIC Evacuation Plans, STIC Daily Command Briefing)

II.C. Criminal Intelligence Analyst (CIA) - Full-time Illinois State Police Code employee who primarily researches and analyzes data in regard to criminal activity, suspects and incidents.

II.D. For Official Use Only (FOUO):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. Information impacting the National Security of the United States and classified Confidential, Secret, or Top Secret under Executive Order 12958, "Classified National Security Information," as amended, or its predecessor or successor orders, is not to be considered FOUO. FOUO is not to be considered classified information.

II.E. Law Enforcement Sensitive (LES): (Middle level unclassified but sensitive information). The term used within STIC to identify unclassified information of a sensitive nature which should not be disseminated outside the scope of law enforcement personnel. LES is 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 and/or State programs, or other programs or operations essential to the national interest. (examples: STIC Daily Intelligence Notes, STIC Event/Group/Target/Method threat assessments).

II.F. Need-to-know: The determination made by an authorized holder of information that 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.

II.G. Protected Critical Infrastructure Information (PCII):Critical infrastructure information (CII) is defined in 6 U.S.C. 131(3) (Section 212(3) of the Homeland Security Act). Critical infrastructure information means information related to the security of critical infrastructure or protected systems not customarily in the public domain. Protected Critical Infrastructure Information is a subset of CII that is voluntarily submitted to the Federal Government and for which protection is requested under the PCII program by the requestor.

II.H. Terrorism Research Specialist (TRS) - Full-time Illinois State Police Code employee who researches and analyses data in regard to potential terrorism suspects and incidents which may be precursors for terrorist activity.

III. RESPONSIBILITIES

III.A. STIC Bureau Chief and Assistant Bureau Chief(s) will:

III.A.1. Be responsible for practical application of all aspects of the program to protect unclassified but sensitive information.

III.A.2. Facilitate center-wide policy guidance.

III.A.3. Take appropriate corrective actions, to include administrative or disciplinary action as appropriate, when violations occur.

III.B. STIC Watch Officers will:

III.B.1. Ensure compliance with the standards for safeguarding sensitive but unclassified information as cited in this directive.

III.B.2. Ensure that an adequate level of education and awareness is established and maintained that serves to emphasize safeguarding and

prevent unauthorized disclosure of unclassified but sensitive information.

III.C. STIC employees, contractors, consultants and others to whom access is granted will:

III.C.1. Be aware of and comply with the safeguarding requirements for unclassified but sensitive information as outlined in this directive.

III.C.2. Be aware that divulging information without proper authority could result in administrative or disciplinary action.

III.C.3. Receive training on safeguarding sensitive information. Upon completion of training, Non-Disclosure Agreements will be read, agreed upon, and signed.

IV. LEVELS OF UNCLASSIFIED BUT SENSITIVE INFORMATION

IV.A. Information Designated as FOUO (For Official Use Only)

Within STIC, the caveat "FOR OFFICIAL USE ONLY" will be used to identify sensitive but unclassified information which can be disseminated outside the scope of law enforcement personnel; however, the information should be considered sensitive and release to the general public is not authorized. FOUO is not otherwise specifically described and governed by statute or regulation. The use of these and other approved caveats will be governed by the statutes and regulations issued for the applicable category of information.

IV.A.1. The following types of information will be treated as FOUO information.

IV.A.1.a. Information that is exempt under the Freedom of Information Act

IV.A.1.b. Information exempt from disclosure per the Privacy Act of 1974

IV.A.1.c. Information, including banking and financial data, protected by statute, treaty, regulation or other written agreements

IV.A.1.d. Information that could be sold for profit

IV.A.1.e. Information that could result in physical risk to personnel

IV.A.1.f. Information revealing security vulnerabilities of critical infrastructure systems, facilities or persons

IV.A.1.g. Information that could threaten federal, state or local government operations security

IV.A.1..h. Information on technologies that could compromise a technological system or cause a denial of service

IV.B. Information designated as FOUO will be sufficiently labeled so that persons having access to it are aware of its sensitivity and protection requirements.

IV.C. Materials containing specific types of FOUO may be further labeled with the applicable caveat, e.g., "Law Enforcement Sensitive," in order to alert the reader of the type of information conveyed.

IV.D. Computer storage media containing FOUO information will be marked "FOR OFFICIAL USE ONLY."

IV.E. FOUO information will not be disseminated in any manner - orally, visually or electronically - to unauthorized personnel.

IV.F. Access to FOUO information is based on "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 of the information will request dissemination instructions from their next-level supervisor or the information's originator.

IV.G. FOUO Markings

IV.G.1 Information designated as FOUO will be sufficiently marked so that persons having access to it are aware of its sensitivity and protection requirements. The lack of FOUO markings on materials does not relieve the holder from safeguarding responsibilities. Where the FOUO marking is not present on materials known by the holder to be FOUO, the holder of the material will protect it as FOUO. Other sensitive information protected by statute or regulation will be marked in accordance with the applicable guidance for that type of information. Information marked in accordance with the guidance provided for the type of information need not be additionally marked FOUO.

IV.G.2 Prominently mark the bottom of the front cover, first page, title page, back cover and each individual page containing FOUO information with the caveat "FOUO."

IV.G.3 Materials containing FOUO information may cite additional access and dissemination restrictions. For example:

This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Illinois State Police (ISP) STIC policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

IV.G.4 Materials being transmitted to recipients outside of STIC, for example, other federal agencies, state or local officials, etc. who may not be aware of what the FOUO caveat represents, shall include the following notice:

This document is FOR OFFICIAL USE ONLY (FOUO). This message and all other messages shared, posted or communicated are prohibited from being re-published in any other forum, discussion or communication, in part or whole, without authorization of the Statewide Terrorism & Intelligence Center (877-ILL-STIC).

IV.G.5 Portions of the document, i.e., subjects, titles, paragraphs, and subparagraphs that contain only For Official Use Only information will be marked with the abbreviation, FOUO.

IV.G.6 Designator or originator information and markings, downgrading instructions, and date/event markings are not required.

IV.H. FOUO information may be shared with other agencies, federal, state, tribal, or local government and law enforcement officials, provided a specific need-to-know has been established and the information is shared in furtherance of a coordinated and official governmental activity. A security clearance is not required for access to FOUO information.

IV.I. In compliance with Department of Homeland Security guidelines:

IV.I.1. FOUO information will not be sent to non governmental email accounts.

IV.I.2 FOUO information will not be posted on any public website.

IV.I.3. FOUO information may be posted on a government controlled or sponsored protected encrypted data network, such as Homeland Security Information Network (HSIN).

IV.J. FOUO material will be destroyed, when no longer needed, as follows:

IV.J.1. Hard copy materials will be destroyed consistent with the Personal Information Protection Act (PIPA).

IV.J.2. Electronic storage media shall be sanitized appropriately by overwriting or degaussing. Contact the Illinois State Police Computer Forensics Unit personnel for additional guidance.

IV.K. Incident Reporting

IV.K.1. Any STIC employee who becomes aware of the loss, compromise, suspected compromise or unauthorized disclosure of FOUO information will notify a Watch Officer.

IV.K.2. Suspicious or inappropriate requests for information by any means, e.g., email or verbal, shall be reported to a Watch Officer.

IV.K.3. Notifications up the Chain of Command to management personnel will be made without delay when the disclosure or compromise of FOUO information could result in physical harm to an individual or compromise a planned or on-going operation.

IV.L Information Designated as LES (Law Enforcement Sensitive)

Information designated as LES will be sufficiently marked so that persons having access to it are aware of its sensitivity and protection requirements. The lack of LES markings on materials does not relieve the holder from safeguarding responsibilities. Where the LES marking is not present on materials known by the holder to be LES, the holder of the material will protect it as LES. Other sensitive information protected by statute or regulation will be marked in accordance with the applicable guidance for that type of information. Information marked in accordance with the guidance provided for the type of information need not be additionally marked LES.

IV.L.1. The following types of information will be treated as LES:

IV.L.1.a Information of a sensitive nature that should not be disseminated outside the scope of law enforcement personnel

IV.L.1.b Information not otherwise categorized by law or statute, the unauthorized disclosure of which could adversely impact a person's privacy or welfare

IV.L.1.c Information not otherwise categorized by law or statute, the unauthorized disclosure of which could adversely impact the conduct of Federal or State programs

IV.L.1.d Information not otherwise categorized by law or statute, the unauthorized disclosure of which could adversely impact programs or operations essential to the national interest

IV.L.1.e Examples of LES information include STIC Daily Intelligence Notes, STIC Event/Group/Method threat assessments, et al

IV.L.2 LES Markings

IV.L.2.a Prominently mark the bottom of the front cover, first page, title page, back cover and each individual page containing LES information with the caveat "LES."

IV.L.2.b Materials being transmitted to recipients outside of STIC, for example, other federal agencies, state or local officials, etc. who may not be aware of what the LES caveat represents, shall include the following notice:

The material contained in this document is LAW ENFORCEMENT SENSITIVE (LES) and cannot be released to non-law enforcement parties, in part or whole, without authorization of the Statewide Terrorism & Intelligence Center (877-ILL-STIC).

IV.L.2.c Computer storage media, i.e., disks, tapes, removable drives, etc., containing confidential information will be marked "LAW ENFORCEMENT SENSITIVE."

IV.L.2.d Portions of the document, i.e., subjects, titles, paragraphs, and subparagraphs that contain only Law Enforcement Sensitive information will be marked with the abbreviation, LES

IV.L.2.e. Designator or originator information and markings, downgrading instructions, and date/event markings are not required.

IV.M. Information Designated as Confidential

Information designated as CONFIDENTIAL will be sufficiently marked so that persons having access to it are aware of its sensitivity and protection requirements. The lack of CONFIDENTIAL markings on materials does not relieve the holder from safeguarding responsibilities. Where the CONFIDENTIAL marking is not present on materials known by the holder to be CONFIDENTIAL, the holder of the material will protect it as

CONFIDENTIAL. Other sensitive information protected by statute or regulation will be marked in accordance with the applicable guidance for that type of information. Information marked in accordance with the guidance provided for the type of information need not be additionally marked CONFIDENTIAL.

IV.M.1 The following types of information will be designated as Confidential:

IV.M.1.a Information of a sensitive nature meant to have limited dissemination

IV.M.1.b Information intended to be disseminated only to STIC, Illinois State Police (ISP), or other entities specifically granted access

IV.M.1.c Information of a confidential nature related to STIC or ISP operational security, personnel, policy decisions, and analytical products still under development

IV.M.1.d Examples of Confidential information include STIC Evacuation Plans, STIC Daily Command Briefing, et al.

IV.M.2. CONFIDENTIAL Markings

IV.M.2.a. Prominently mark the bottom of the front cover, first page, title page, back cover and each individual page containing CONFIDENTIAL information with the caveat "CONFIDENTIAL."

IV.M.2.b. Materials being transmitted to recipients outside of STIC, for example, other federal agencies, state or local officials, etc. who have been granted access to ISP STIC confidential material should be further advised as to what the CONFIDENTIAL caveat represents:

This document contains Illinois State Police (ISP) Statewide Terrorism & Intelligence Center (STIC) CONFIDENTIAL information. It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance to STIC policy relating to CONFIDENTIAL information. Disclosure of this information to parties other than ISP, STIC, or others

to whom access is granted, may affect operational security, personnel security, or on-going analytical products not yet meant to be disseminated outside of said parties.

IV.M.2.c. Computer storage media, i.e., disks, tapes, removable drives, etc., containing confidential information will be marked "CONFIDENTIAL."

IV.M.2.d. Portions of the document, i.e., subjects, titles, paragraphs, and subparagraphs that contain only confidential information will be marked with the term (CONFIDENTIAL).

IV.M.2.e. Designator or originator information and markings, downgrading instructions, and date/event markings are not required.

IV.N. Non-Departmental Devices

IV.N.1. The processing, storage, copying or duplication of any official STIC information, request, assessment, report or document will be accomplished using only STIC provided or authorized devices and only in the furtherance of official duties.

IV.N.2. The possession and/or use of a non-departmental computer (i.e. not issued by STIC or the Illinois State Police, either a laptop or desktop) is strictly prohibited within the STIC Watch Center without the expressed written permission of a STIC Watch Officer or the Center Chief or Assistant Center Chief.

IV.N.3. The possession and/or use of any non-departmental storage device (including but not limited to jump/thumb/key drives, memory sticks, iPods, interface capable PDAs, storage media (floppy/cd/dvd/zip disks), or digital or film cameras) is strictly prohibited within the STIC Watch Center without the expressed written permission of a STIC Watch Officer or the Center Chief or an Assistant Center Chief.

IV.N.4. The possession and/or use of any non-departmental cell-phone with camera functionality or removable storage media is strictly prohibited within the STIC Watch Center without the expressed written permission of a STIC Watch Officer or the Center Chief or an Assistant Center Chief.

IV.N.5. When any of the above devices or types of storage media are brought into the STIC Watch Center, such devices or storage media may be confiscated and examined to ensure they are not being used to copy or store any unauthorized STIC information or materials. Examination may include a forensic exam of the device or storage media.

V. GENERAL POLICY AND PROCEDURES

V.A. The Computer Security Act of 1987, Public Law 100-235, defines "sensitive information" as "any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under Section 552a of Title 5, United States Code (the Privacy Act) but which has not been specifically authorized under criteria established by an executive order or an act of Congress to be kept secret in the interest of national defense or foreign policy." However, with the exception of certain types of information protected by statute, specific, standard criteria and terminology defining the types of information warranting designation as "sensitive information" does not exist within the Federal or State government. Such designations are left to the discretion of each individual agency.

V.B. Within the "sensitive but unclassified" arena, in addition to the various categories of information specifically described and protected by statute or regulation, e.g., Tax Return Information, Privacy Act Information, Sensitive Security Information (SSI), Critical Infrastructure Information (CII), Grand Jury Information, etc. There are numerous additional caveats used by various agencies to identify unclassified information as sensitive, e.g., For Official Use Only; Law Enforcement Sensitive; Official Use Only; Limited Official Use; etc. Regardless of the caveat used to identify it, however, the reason for the designation does not change. Information is designated as sensitive to control and restrict access to certain information, the release of which could cause harm to a person's privacy or welfare, adversely impact economic or industrial institutions, or compromise programs or operations essential to the safeguarding of our national interests.

V.C. Designation of information as CONFIDENTIAL, LES, or FOUO is not a vehicle for concealing government negligence, ineptitude, illegalities, or other disreputable circumstances embarrassing to a government agency.

V.D. Some types of unclassified but sensitive information may be more sensitive than others and thus warrant additional safeguarding measures beyond the minimum requirements established in this manual. For example, certain types of information may be considered extremely sensitive based on the repercussions that could result should the information be released or compromised. Such repercussions could be the loss of life or compromise of an informant or operation. Additional control

requirements may be added as necessary to afford appropriate protection to the information. ISP STIC employees, contractors, and detailees must use sound judgment coupled with an evaluation of the risks, vulnerabilities, and the potential damage to personnel or property as the basis for determining the need for safeguards in excess of the minimum requirements and protect the information accordingly.

V.D.1. When removed from an authorized storage location and persons without a need-to-know are present, or where casual observation would reveal CONFIDENTIAL, LES, or FOUO information to unauthorized persons, an appropriate cover sheet entitled "Confidential," "Law Enforcement Sensitive," or "For Official Use Only" (See attached STIC Cover sheet examples) will be used to prevent unauthorized or inadvertent disclosure.

V.D.2. When forwarding unclassified but sensitive information, the appropriate cover sheet should be placed on top of the transmittal letter, memorandum or document.

V.D.3. When receiving unclassified but sensitive information from another government agency, handle in accordance with the guidance provided by the other government agency. Where no guidance is provided, handle in accordance with the requirements of this directive. If the guidance is less than the minimum STIC procedures, follow the minimum STIC procedures outlined in this directive.

V.E. General Marking Procedures

V.E.1. Information designated as CONFIDENTIAL, LES, or FOUO will be sufficiently marked so that persons having access to it are aware of its sensitivity and protection requirements. The lack of markings on materials does not relieve the holder from safeguarding responsibilities. Where a marking is not present on materials known by the holder to be unclassified but sensitive, the holder of the material will protect it as outlined in this directive. Other sensitive information protected by statute or regulation will be marked in accordance with the applicable guidance for that type of information. Information marked in accordance with the guidance provided for the type of information need not be additionally marked CONFIDENTIAL, LES, or FOUO.

V.E.2. Information and analytical products produced by STIC should be designated as CONFIDENTIAL, LES, or FOUO. The highest designation should be prominently marked on the front cover (if applicable), first page (under title),and each page in the header or footer sections. Portions of the document, i.e., subjects, titles, paragraphs, and subparagraphs that contain only CONFIDENTIAL, LES, or FOUO information will be marked at the beginning of the segment with the appropriate abbreviation.

V.F. Designation Authority

Any STIC employee, detailee, or contractor who has received training on how to safeguard information can designate information as CONFIDENTIAL, LES, or FOUO. Officials occupying supervisory or managerial positions are authorized to designate other information, not listed above and originating under their jurisdiction, as CONFIDENTIAL, LES, or FOUO.

V.G. Duration of Designation

Information designated as CONFIDENTIAL, LES, or FOUO will retain its designation until determined otherwise by the originator or a supervisory or management official having program management responsibility over the originator and/or the information.

V.H. Dissemination and Access

V.H.1. Unclassified but sensitive information will not be disseminated in any manner - orally, visually, or electronically - to unauthorized personnel.

V.H.2. Access to unclassified but sensitive information is based on "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 of the information will request dissemination instructions from their next-level supervisor or the information's originator.

V.H.3. The holder of the information will comply with any access and dissemination restrictions.

V.H.4. A background security clearance is not required for access to FOUO information. A background security clearance by the Illinois State Police, federal agency, or other governmental agency is required for CONFIDENTIAL and LES information.

V.H.5. When discussing or transferring unclassified but sensitive information to another individual(s), ensure that the individual with whom the discussion is to be held or the information is to be transferred has a valid need-to-know, and that precautions are taken to prevent unauthorized individuals from overhearing the conversation, observing the materials, or otherwise obtaining the information

V.H.6. Unclassified but sensitive information may be shared with other agencies, federal, state, tribal, or local government and law enforcement officials, provided a specific need-to-know has been established and the information is shared in furtherance of a coordinated and official governmental activity. Where such information is requested by an official of another agency and there is no coordinated or other official governmental activity, a written request will be made from the requesting agency to the STIC supervisory personnel providing the name(s) of personnel for whom access is requested,

the specific information to which access is requested, and basis for need-to-know. The STIC supervisor shall then determine if it is appropriate to release the information to the other agency official. When such information is released, appropriate cover sheets are mandated.

V.H.7. Other sensitive information protected by statute or regulation, i.e., Privacy Act, CII, SSI, Grand Jury, etc., will be controlled and disseminated in accordance with the applicable guidance for that type of information.

V.H.8. If the information requested or to be discussed belongs to another agency or organization, comply with that agency's policy concerning third party discussion and dissemination

V.I. Storage

V.I.1. When unattended, unclassified but sensitive materials will, at a minimum, be stored in a locked or unlocked file cabinet, locked desk drawer, a locked overhead storage compartment such as a systems furniture credenza, or similar compartment at ISP facilities. Materials 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 a need-to-know, such as a locked room, or an area where access is controlled by a guard, cipher lock, or card reader.

V.I.2. Unclassified but sensitive information will not be stored in the same container used for the storage of classified information unless there is a correlation between the information. When such materials are stored in the same container used for the storage of classified materials, they will be segregated from the classified materials to the greatest extent possible, i.e. separate folders, separate drawers, etc. This restriction is due to the possible misinterpretation of classified material as CONFIDENTIAL, LES, or FOUO. Classified materials will not be handled outside the closed secure storage facility where classified federal databases will be located. These classified materials will be secured in the safe within the closed secure storage facility.

V.I.3. Unclassified but sensitive information must be stored on secure, State of Illinois Central Management Services (CMS) computers and servers. Secure firewalls must be in place and computers must have up-to-date internet security programs with the inclusion of anti-virus and anti-spy ware software.

V.I.4. Laptop computers and other media containing unclassified but sensitive information will be stored and protected to prevent loss, theft, unauthorized access and unauthorized disclosure. Media containing CONFIDENTIAL, LES, or FOUO information shall be clearly marked.

V.J. Transmission

V.J.1. Transmission of hard copy unclassified but sensitive information within the U. S. and its Territories:

V.J.1.a. Material will be placed in a single opaque envelope or container and sufficiently sealed to prevent inadvertent opening and to show evidence of tampering. The envelope or container will bear the complete name and address of the sender and addressee, to include program office and the name of the intended recipient (if known).

V.J.1.b. Unclassified but sensitive materials may be mailed by U. S. Postal Service First Class Mail or an accountable commercial delivery service such as Federal Express (FedEx) or United Parcel Service (UPS).

V.J.1.c. Unclassified but sensitive materials may be entered into an inter-office mail system provided it is afforded sufficient protection to prevent unauthorized access, e.g., sealed envelope.

V.J.2. Transmission to Overseas Agencies (if applicable): When an overseas office is serviced by a military postal facility (i.e., APO/FPO), CONFIDENTIAL, LES, or FOUO may be transmitted directly to the office. Where the overseas office is not serviced by a military postal facility, the materials will be sent through the Department of State, Diplomatic Courier.

V.J.3. Electronic Transmission.

V.J.3.a. Transmittal via Fax. Unless otherwise restricted by the originator, unclassified but sensitive information may be sent via non-secure fax. Where a non-secure fax is used, the sender will coordinate with the recipient to ensure CONFIDENTIAL, LES, or FOUO guidelines are followed. The holder of the material will comply with any access, dissemination, and transmittal restrictions cited on the material or verbally communicated by the originator.

V.J.3.b. Transmittal via E-Mail: Unclassified but sensitive information transmitted via email should be protected by encryption or transmitted within secure communications systems. When this is impractical or unavailable, unclassified but sensitive may be transmitted over regular email channels. For added security, when transmitting unclassified but sensitive over a regular email channel, the information can be included as a password protected attachment with the password provided under separate cover. Recipients of

unclassified but sensitive information will comply with any email restrictions imposed by the originator.

V.J.3.c. State of Illinois Internet/Intranet

V.J.3.c.i Unclassified but sensitive information will not be posted on a State of Illinois or any other internet (public) website.

V.J.3.c.ii. Unclassified but sensitive information may be posted on the State of Illinois intranet or other government controlled or sponsored protected encrypted data networks, such as the Homeland Security Information Network (HSIN) and the Joint Regional Information Exchange System (JRIES). However, the official authorized to post the information should be aware that access to the information is open to all personnel who have been granted access to that particular intranet site. The official must determine the nature of the information is such that need-to-know applies to all personnel; the benefits of posting the information outweigh the risk of potential compromise; the information posted is prominently marked as "CONFIDENTIAL," "LAW ENFORCEMENT SENSITIVE," OR "FOR OFFICIAL USE ONLY;" and information posted does not violate any provisions of the Privacy Act.

V.K. Incident Reporting

V.K.1. The loss, compromise, suspected compromise, or unauthorized disclosure of unclassified but sensitive information will be reported. Incidents involving unclassified but sensitive information in STIC IT systems will be reported to STIC supervisory personnel.

V.K.2. Suspicious or inappropriate requests for information by any means, e.g., email or verbal, shall be report to STIC supervisory personnel.

V.K.3. Employees or contractors who observe or become aware of the loss, compromise, suspected compromise, or unauthorized disclosure of unclassified but sensitive information will report it immediately, but not later than the next duty day, to the originator and STIC supervisory personnel.

V.K.4. Additional notifications to appropriate ISP management personnel will be made without delay when the disclosure or compromise could result in physical harm to an individual(s) or the compromise of a planned or on-going operation.

V.K.5. An inquiry may be conducted by STIC supervisory personnel or other designee to determine the cause and effect of the incident and the appropriateness of administrative or disciplinary action against the offender.