ILLINOIS STATE POLICE DIRECTIVE
SRV-226, INFRASTRUCTURE SECURITY AWARENESS (ISA) PROGRAM

RESCINDS: New Directive	**REVISED:** 08-30-2021 **2021-021**
RELATED DOCUMENTS:	**RELATED CALEA STANDARDS (6th Edition):** 40.2.1, 40.2.2, 40.2.3, 43.1.2, 46.2.6, 82.1.1

I. POLICY

The Illinois State Police (ISP) Statewide Terrorism and Intelligence Center (STIC) will maintain an Infrastructure Security Awareness (ISA) Program for participating entities located in or having a nexus to Illinois responsible for the protection of physical and cyber critical infrastructure within the United States. The ISA Program was designed to share vital, For Official Use Only (FOUO) information and ensure timely dissemination of critical infrastructure protection guidance and intelligence with those who have a 'need to know.' These member entities can also report FOUO information to STIC.

II. AUTHORITY

II.A. 28 Code of Federal Regulations Part 23 (28 CFR Part 23)

II.A.1. 28 CFR Part 23 provides guidance to law enforcement regarding how to operate criminal intelligence information systems effectively while safeguarding privacy and civil liberties. The regulation helps protect an individual's privacy and constitutional rights during the collection, storage, and dissemination of criminal intelligence information.

II.A.2. The ISA Program collects and shares intelligence-related information under 28 CFR Part 23 guidelines.

II.B. 5 U.S.C. § 552, Federal Freedom of Information Act (FOIA)

II.B.1. Any person has the right to request access to federal agency records or information except to the extent the records are protected from disclosure by any of nine exemptions contained in the law or by one of three special law enforcement record exclusions.

II.B.2. Exemptions of this Act include:

II.B.2.a. Classified information for national defense or foreign policy;
II.B.2.b. Internal personnel rules and practices;
II.B.2.c. Information that is exempt under other laws;
II.B.2.d. Trade secrets and confidential business information;
II.B.2.e. Inter-agency or intra-agency memoranda or letters that are protected by legal privileges;
II.B.2.f. Personnel and medical files;
II.B.2.g. Law enforcement records or information;
II.B.2.h. Information concerning bank supervision; and
II.B.2.i. Geological and geophysical information.

II.B.3. Information designated as FOUO and shared with STIC is not automatically exempt from disclosure under 5 U.S.C. § 552, Federal Freedom of Information Act. Information requested by the public under a FOIA request must still be reviewed on a case-by-case basis.

II.C. 5 ILCS 140/Illinois Freedom of Information Act (FOIA)

II.C.1. Each public body shall make available to any person for inspection or copying all public records, except as otherwise provided in Section 7 of this Act. Notwithstanding any other law, a public body may not grant to any person or entity, whether by contract, license, or otherwise, the exclusive right to access and disseminate any public record as defined in this Act.

II.C.2. Exemptions of this Act include:

II.C.2.a. Information specifically prohibited from disclosure by federal or state law or rules and regulations adopted under federal or state law.

II.C.2.b. Information that, if disclosed, would constitute a clearly warranted invasion of personal privacy, unless the disclosure is consented to in writing by the individual subjects of the information. The disclosure of information that bears on the public duties of public employees and officials shall not be considered an invasion of personal privacy.

II.C.2.c. Information designated as FOUO and shared with STIC is not automatically exempt from disclosure under 5 ILCS 140/Freedom of Information Act.

II.D. STIC Privacy Policy

II.D.1. Internal operating policy which outlines how personally identifiable information is collected, used, and secured by STIC.

II.D.1.a. STIC standard operating procedures and policies have been adopted to comply with federal and Illinois law concerning the appropriate collection, analysis, dissemination and retention of personally identifiable information and intelligence data.

II.D.1.b. Reports regarding alleged violations and suggestions for amendments shall be submitted to the Illinois State Police Privacy Office.

III. DEFINITIONS

III.A. Participating Entity - private sector professionals and/or organizations that share with and receive homeland security awareness, prevention, response, mitigation and recovery information from STIC. These entities are located in Illinois or have an Illinois nexus. A distribution list of participating entities is maintained by STIC for the purpose of dissemination of information.

III.B. Critical Infrastructure - assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof [Department of Homeland Security (DHS) definition].

III.C. For Official Use Only (FOUO) - unclassified sensitive information that may be exempt from mandatory release to the public under the FOIA. Information is not otherwise categorized by statute or regulation. Unauthorized disclosure of FOUO information could adversely impact a person's privacy or welfare, the conduct of federal or state programs, or other programs or operations essential to the national interest.

III.D. Need to Know - established when the prospective recipient requires access to specific information in order to perform their job protecting critical infrastructure and key resources.

III.E. Secret Level Information Classification - information that could reasonably be expected to cause serious damage to national security under unauthorized disclosure.

III.F. Security Screening - includes searches of the following databases:

III.F.1. Vital

III.F.2. Open Source

III.F.3. Illinois Secretary of State Corporation/Limited Liability Corporation (LLC) Search/Certificate of Good Standing

III.F.4. Clear

III.F.5. Indices, excluding Criminal History Record Information (CHRI) and Firearm Owners Identification (FOID)

III.F.6. TransUnion TLOxp

III.F.7. DHS security screening for Secret Level Security Clearance (if applicable)

III.G. Derogatory Information - negative information retrieved during the security screening process of program applicants related to criminal histories.

IV. PROCEDURES

IV.A. The ISP, STIC, Division of Criminal Investigation (DCI) will:

IV.A.1. Maintain procedures for processing applications to the ISA Program.

IV.A.1.a. Receives requests for membership in the ISA Program.
IV.A.1.b. Provides program application and Non-Disclosure Agreement (NDA) documentation.
IV.A.1.c. Reviews completed program application and NDA to ensure eligibility and acknowledgement of rules for program participation.
IV.A.1.d. Performs a security screening on the applicant.

IV.A.1.d.1) Applicants may be disqualified for program membership if specific derogatory information is found. However, the following will not automatically disqualify the applicant:

IV.A.1.d.1)a) Arrests without convictions for misdemeanors.
IV.A.1.d.1)b) Convictions for misdemeanors where an acceptable length of time has passed.

IV.A.1.d.2) Discretion may be used at any time during the membership decision approval.

IV.A.1.e. Handles reports and requests for information from vetted private sector entities.

IV.A.2. Conduct an annual program audit to ensure compliance with all guidelines of the ISA Program.

IV.A.2.a. An annual compliance reminder will be sent to all members of the program that will require the acknowledgement of the information sharing guidelines established in the NDA.
IV.A.2.b. Members who violate the program guidelines are subject to removal from the program.

IV.A.3. Maintain procedures for collection of intelligence information from ISA participating entities.

IV.A.3.a. All intelligence information collection will comply with 28 CFR Part 23 guidelines.
IV.A.3.b. All intelligence information collection will comply with the STIC Privacy Policy.
IV.A.3.c. Vetted private sector entities may report criminal activity or suspicious incidents to STIC. STIC will handle the information in accordance with 28 CFR Part 23 and the STIC Privacy Policy. STIC will analyze the information and will share with local, state, and federal law enforcement, if necessary.

IV.A.4. Maintain procedures for dissemination of intelligence information to ISA distribution list.

IV.A.4.a. Unclassified FOUO and open source information will be shared with vetted participating entities.
IV.A.4.b. Vetted partners with a valid secret security clearance are eligible to participate in classified briefings hosted by STIC.
IV.A.4.c. Verification of secret clearances will be conducted before each briefing for each member that indicates participation.

IV.B. ISA Program Manager will:

IV.B.1. Notify applicants who are accepted into the program. Applicants who do not qualify for program membership will not be notified. Some specific derogatory information does not mean an applicant does not qualify for program membership.

IV.B.2. Maintain program membership lists and manage the probate sector distribution list.

IV.B.3. Serve as the point of contact for vetted private sector entities.

IV.B.4. Share FOUO information with vetted private sector entities.

IV.B.5. Conduct an annual membership audit by January 31 of each year.

IV.C. STIC Assistant Center Chief will:

IV.C.1. Manage the activities of the ISA Program and the program manager.

IV.C.2. Serve as a first line supervisor for the ISA Program Manager.

IV.C.3. Establish strategies and assignments in support of the strategic planning process for the ISA Program.

-End of Directive-