ADVISORY: Records Retention, Records Schedules, and Privacy Notices for Insider Threat-Related Information

NITTF – ADV – 2014 – 002

DATE: 2 May 2014

PURPOSE:

As departments and agencies (D/A) build insider threat programs, those programs will be required to gather different kinds of insider threat-related information for analysis and appropriate action. Questions may arise pertaining to the use and retention of that information. This advisory note provides D/A insider threat programs with guidance to assist in the proper management of insider threat-related information.

GUIDANCE:

In establishing insider threat programs, or revamping existing information assurance or personnel security alert/investigatory activities in implementing new insider threat directives and standards, agency officials and program managers must take care to engage their legal counsel, privacy and civil liberties officers, and information management experts regarding the collection, maintenance and sharing of relevant records.

Records that are generated and administered in the course of Insider Threat program activities (e.g., records about individuals' use of government equipment) are the subject of certain public notices mandated by the Privacy Act (i.e., Systems of Records Notices, or SORNs) if they are maintained and retrieved by an individual's name or unique identifier. Additionally, these program records constitute "federal records" subject to "scheduling" by the National Archives and Records Administration (NARA) pursuant to the Federal Records Act. NARA prescribes the period of time and manner in which particular types of records shall be retained. Depending how the individual D/A is implementing its Insider Threat program, there already may exist applicable Privacy Act notices and NARA-approved schedules that need only be amended. On the other hand, it may be necessary to develop and obtain approval for new Privacy Act or Federal Records Act documentation consistent with program activities. Accordingly, it is critical that you enlist the expertise resident in your agencies in meeting these requirements.

It is the D/A's responsibility to ensure proper disposition of records collected or generated for insider threat-related activities. Each D/A has an Information Management Office that can assist in determining the appropriate Records Control Scheduling (RCS) for its insider threat information. If there is no NARA-approved RCS suitable for the insider threat-related records, the D/A Information Management Office will propose a new RCS (or schedules) for NARA approval. While a new RCS is pending with NARA, all records should be retained. (D/As should consult with their Office of General Counsel and Information Management Office if indefinite retention conflicts with other applicable retention regimes.)

If insider threat-related records are retrieved from D/A files (whether paper or electronic) by an employee's name or unique personal identifier, the D/A must determine whether current agency SORNs adequately cover these records, or if a new SORN or SORNs must be published. If there exists a SORN for one type of record utilized for insider threat purposes, but not for another, the D/A can proceed with those aspects of the "program" for which a SORN(s) exists. The D/A may not collect the type of record for which there is no SORN until an appropriate SORN is published. Expertise on SORNs and other Privacy Act requirements is available through D/A Civil Liberties and Privacy Offices and Offices of General Counsel.

NITTF POC: If you have questions regarding this Advisory, please send your request to (b)(3) (b)(3)

(b)(3)(b)(6)