www.ncix.gov\nittf\index.php

ADVISORY: Legal Guidance on Insider Threat Program Issues

NITTF – ADV– 2014 – 001

DATE: 2 May 2014

BACKGROUND: On 24 January 2014 the NITTF hosted one of its continuing series of legal panel discussions. Attendees at the event, which was held at the Department of Justice, were General Counsel representatives, Privacy and Civil Liberties officials, and Whistleblower Protection officials from within the departments and agencies that handle classified information. Since the previous May 2013 Legal Forum, the NITTF had accumulated questions pertaining to the establishment of insider threat programs and the conduct of insider threat activities under Executive Order 13587 and the National Insider Threat Policy and Minimum Standards. The 24 January 2014 panel discussion provided an opportunity for panelists to offer remarks pertaining to the various questions and for the audience to engage in discussions on those points with the panelists. The following is a summary of the remarks of the panel members on the topics that were discussed during the forum. This written guidance has all been vetted with the originators to ensure consistency with their oral remarks.

PURPOSE: The written guidance here does not represent policy pronouncements but, rather, the best professional advice that can be assembled from legal and professional experts who engage daily in insider threat issues. It is presented in a Question and Answer format for ease of use. Ultimately, each individual department and agency must employ its own legal counsel and privacy and civil liberties officials to guide the path of the organization in insider threat matters. This Advisory is intended to assist in providing that guidance. This Advisory applies to Executive Branch Departments and Agencies subject to Executive Order (EO) 13587, Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information.

GUIDANCE:

Insider Threat Authority--

--Discuss situations in which a member of an agency insider threat program might exceed his/her department's or agency's (D/A) authority in an inquiry, in conducting user computer monitoring, in reviewing personal information prior to the establishment of an insider threat inquiry or investigation.

Among the ways a person conducting an inquiry might exceed his/her authority: In computer monitoring, a prime example of exceeding one's authority might be to arrange the emplacement of additional triggers to focus deeper attention on the activities of an individual without that additional scrutiny being part of an approved insider threat inquiry or investigation. In reviewing personal information an insider threat program person might exceed his/her authority by gathering and accessing information on individuals for which there is no logical connection to an insider threat concern or accessing information that is statutorily protected without proper authorization.

--Under what circumstances would an insider threat program person be criminally or civilly liable for exceeding such authority? Are there any circumstances under which the insider threat program employee might be subject to a Bivens action for violating the constitutional rights of a subject?

Based on the individual facts, a program person might be criminally and civilly liable for any of the above actions or for any action that either violated the law (e.g. ECPA or Title III) or was viewed as a negligent act or an act that wilfully violated the trust bestowed on the program person. A federal employee may incur person civil liability for a constitutional tort claim (Bivens action) for conduct that allegedly violates a right secured by the Constitution (e.g. First Amendment; Fourth Amendment). For example, insider threat personnel may face Bivens liability for actions associated with infringing on another's free speech (First Amendment) or conducting an unreasonable search or seizure (Fourth Amendment).

Computer Banners--

--Are banners required on portable devices, such as Blackberries?

The use of banners is required for all classified USG National Security Systems, portable or not. The Minimum Standards require that D/A heads ensure that insider threat programs include classified and unclassified banners informing users that their activity on the network is being

monitored and that all cleared employees must sign an agreement acknowledgment that their activity on any D/A classified or unclassified network, to include portable devises, is subject to monitoring and search.

Monitoring Unclassified Networks--

--Is monitoring of the activities of cleared personnel on unclassified USG computers also permissible under the president's policy and standards?

Yes, while not required, it is permitted. With the proper banner language, there is no reasonable expectation of privacy on any USG system. Also, the Minimum Standards require that all cleared persons acknowledge, in writing, that their activity on any D/A network, to include portable electronic devices, is subject to monitoring and search and that the results could be used for any official government purpose, including but not limited to national security, criminal, security, or administrative investigations or proceedings.

Computer Monitoring of Employees From Another Agency--

--Under what circumstances may an agency conduct computer monitoring on another agency's employee? For example, if an agency provides the network service to another agency, may the first agency conduct monitoring for the second agency? If so, are there any limitations or considerations that must be taken into account? If an agency collects monitoring data on another agency's employee, is the collecting agency obligated to send the information to the employee's parent agency? Are there any limits on what the collecting agency is allowed to do with this information?

As long as the monitoring agency has a valid USG purpose to conduct the monitoring, that monitoring can legally extend to federal persons outside the monitoring agency who are given access to the USG computer system being monitored.

By mutual agreement two D/A may agree that one D/A will monitor the computer activities of the second D/A on a particular network.

There is presently no requirement for an agency that is collecting monitoring results on persons from another D/A to provide those results to that D/A. The sharing of such results, however, can be arranged by mutual agreement.

Establishing Procedures for Computer Monitoring--

--Which are the best legal "vehicles" for establishing authority for an insider threat computer monitoring program (i.e., is internal agency regulation sufficient or is notice and comment rulemaking under the Administrative Procedures Act necessary)?

Internal D/A procedures are sufficient. No rulemaking is required or necessary. D/A should review their Privacy Act System of Records Notice(s) to ensure that the SORN(s) covers the information that the agency is collecting under the authority of their insider threat programs.

Limitations on Computer Monitoring--

--What, if any, limits do you see from a legal and privacy-civil liberties perspective on a D/A's authority to monitor the activities of its cleared employees on government computers?

The USG cannot be capricious or arbitrary in its actions. It may conduct what monitoring its insider threat program deems necessary, in whatever order and to whatever degree of detail, so long as that monitoring is not arbitrary. To establish the rationale for differing degrees or patterns of monitoring, the D/A should establish a set of monitoring protocols and procedures that will apply.

--If an agency monitors all of its cleared employees, must it apply all monitoring triggers or indicators against all employees, or may the indicators be tailored based on the different populations within the agency?

No, a D/A need not apply the same triggers to all cleared personnel. It may tailor its monitoring triggers to meet what its insider threat program reasonably believes provides appropriate coverage to a particular population of employees. These triggers should be documented in writing.

Focused Monitoring--

--Once a D/A identifies an employee's activities as a possible insider threat concern, is any special permission or authority required to conduct more precise, focused computer monitoring of that individual in order to gather information to refute or confirm the concern? In other words, can computer monitoring be used as an investigative tool by the agency? To state this differently: is there a legal distinction between authority that exists under which a D/A can conduct user activity monitoring across its entire cleared employee population and the authority that would be necessary to conduct monitoring that focused on the activities of a cleared

employee about whom an insider threat inquiry is being conducted? How should on agency approach the topic of "focused monitoring?"

Extending or deepening user monitoring is a matter for the individual D/A to determine. D/A authorities will probably reside with the insider threat program senior designated official or program manager with procedures for extending coverage set forth in a program SOP. Beyond that, no special authority is required for focused monitoring.

Access to Information by the Insider Threat Program--

--Should the insider threat program insist on information feeds on all cleared personnel from offices across the D/A, or should some attempt be made to limit the information that flows into the program for onalysis until such time as a certain concern threshold has been reached?

There is no legal or policy standard governing this. As a reasonable approach, the D/A insider threat program officials should engage with those D/A stakeholders that "own" the information processes for information desired by the insider threat program. That engagement should seek to identify how much and at what point information should flow into the "hub" for analysis. If too much information is pushed to the "hub," it may drown the hub by virtue of its sheer quantity. If access, however, is made too restrictive, then analysis may be incomplete or flawed. A reasonable, agency-specific approach among stakeholders should prevail.

Access to Employee Assistance Program Files--

--Should an insider threat program have access to an agency's Employee Assistance Program files, including any medical or treatment records that may be contained therein?

There is no legal prohibition to the insider threat program having access to these files and the information contained therein. It is a matter for the D/A head to decide, in consultation with his/her counsel and privacy/civil liberties officials. Rules and procedures governing access to such information should be spelled out in an appropriate D/A procedures manual or standard operating procedure.

Sharing Information on Employees with Another Agency--

--Are there any particular rules or limitations that o D/A must follow when considering whether it will share information about its employees—including the results of insider threat inquiries—with other agencies? What are the statutory authorities for information sharing?

Yes, if personally identifiable information is involved. The Privacy Act contains specific provisions, called Conditions of Disclosure that govern the disclosure of employee information containing personally identifiable information. Each D/A must adhere to these Conditions of Disclosure to share information with others. Consultation with the D/A Privacy and Civil Liberties Office is the surest way to guarantee that information to be shared is shared properly.

Systems of Records Notices--

--Under the Privacy Act, will a Systems of Records Notice (SORN) be required for insider threat records?

If the insider threat records contain information on an individual that can be retrieved by the person's name or an identifier uniquely associated with the individual, then the information constitutes a system of records under the Privacy Act and must be covered by a SORN.

Privacy Act/Freedom of Information Act Requests For Insider Threat Inquiry Files--

--Would there be grounds for someone to request these files? Many of these would be classified, given the nature of the predicating concern. But there could also be an inquiry on a threat to non-classified national security-related information (e.g., border crossing information, aviation records, biological components) in which the inquiry is not classified. Would these records be available?

*Could someone seek these Insider Threat files? Yes, someone could request these records under either the Freedom of Information Act or the Privacy Act, depending on the circumstances and the standing of the requester. The D/A would have to process such requests using their normal procedures for FOIA or Privacy Act decisions. Without going into the intricacies of either statute, the Privacy Act generally permits any individual to request access to and to correct factual errors in their record maintained in an agency's "system of records". The Freedom of Information Act generally requires a D/A to release an agency record upon request of any person.

*How do the rules for a request work? Each request must be analyzed carefully to determine whether to process a request for records under the Privacy Act or Freedom of Information Act. Then, the D/A must follow the laws and the D/A's own published procedures for receiving and searching for records described in the particular type of request, determining if a reason exists to withhold the record, and responding to the requester. It is important to note that both statutes start with the idea that you must disclose the records to a proper

requester, and then the statutes allow withholding a record under very strict "exceptions" or "exemptions." For your D/A procedures, recommend you consult with your agency's Chief FOIA Officer and Chief Privacy Officer, and your legal advisor's office.

*What grounds exist for withholding the record or denying access? Each statute lists limited and technical reasons for withholding. Again, your FOIA or Privacy Act staff can assist you with analyzing if any of these reasons exist. Classification of information is not an automatic grounds for withholding the information in a record. However, classified information in a record can be withheld from a subject's Privacy Act or any person's FOIA requests. Similarly, certain law enforcement or security investigation records could be withheld, depending on the specifics of the case. Both statutes allow a requester to seek judicial remedies for failure to properly deal with a request for release of records. Also, in some instances, D/A officials could face criminal charges for serious failures to comply with the statutes.

Inquiry Guidelines & Limits--

--What are the legal and privacy guidelines or limits governing what an agency can do when conducting an insider threat inquiry or investigation?

A D/A cannot exceed the legal authorities that permit that inquiry. These authorities are implemented through D/A policies or regulations that have been promulgated to govern such inquiries. Internal D/A procedures put in place under existing authorities also will govern the D/A's activities in conducting an inquiry. There are four areas that D/As need to be particularly mindful of:

*First, D/A policies and standards for initiating and conducting inquiries should be tailored to meet mission requirements. The National Insider Threat Policy requires agencies to "employ risk management principles, tailored to meet the distinct needs, mission, and systems of individual agencies." They must also protect privacy and civil liberties. The closer you can tie the efficacy of the measure that you employ with your mission, the less likely you will unduly infringe upon the privacy and civil liberties of your employees.

*Second, you must be particularly aware of policies that could allow—or even appear to allow—agency officials to investigate or collect information regarding an employee solely based on the exercise of constitutionally protected activity (e.g., freedom of speech or religion). This

is consistent with Supreme Court rulings, the Privacy Act (552a(e)(7)), and for Intelligence Community elements, their Attorney General-approved U.S. persons Guidelines.

*Third, when considering privacy and civil liberties and any intrusions on these areas necessary to accomplish the mission, it is "not one or the other." You can and must do both. If the mission requires intrusions, you must balance these intrusions with additional protection and safeguards. For example, if your agency requires some particularly sensitive data, it does not necessarily mean all insider threat personnel should have access to that information. Special access rules can be developed for such information.

*Fourth, it is critical that D/A employees are afforded due process rights in regards to policies and standards. Standards and policies should be clearly drafted. Employees should be provided notice of what is expected of them and when they will be monitored. Note that the National Insider Threat Policy and Minimum Standards require that the individual employee acknowledge this notification in writing. D/A should establish written policies for taking action against employees and employees should be provided notice, in advance if possible, before adverse action is taken against them.

Retaining Records--

--What guidance should a D/A follow with respect to retaining the results of an insider threat inquiry or investigation? How long should results be maintained by the D/A? Should the answer be any different if the results of the inquiry explain or exonerate a subject from any insider threat concern or if the results simply cannot document the insider threat concern? If a person is determined not to be an "insider threat concern," how should the D/A deal with his/her file within the insider threat program?

The insider threat policy and minimum standards do not address specifically how long investigations or inquiries must be retained. Every organization has its own unique authorities and each D/A must assess whether they have the requisite authorities and implementation policies to cover the D/A's needs for insider threat program records. The D/A should look at its operational mission and ask how long, from a mission perspective, should the information be retained. Information analysts will generally say that longer is always better, but the D/A should attempt to quantify the retention period based on need.

To a certain extent, there are existing statutes, executive orders, and internal agency polices that will govern how long a D/A can retain the results of insider threat inquiries or investigations. This is true regardless of whether a threat is determined to be founded, unfounded, or just unknown at this time. Although the statutes and executive orders are unlikely to be changed, they provide a great deal of flexibility in determining a D/A's policies. The D/A's retention policy should be determined by the specific mission of the D/A and must be consistent with agency implementing policies for the Privacy Act. Members of the Intelligence Community must also ensure that their retention policies are consistent with EO 12333 and any applicable Attorney General-approved U.S. persons guidelines for the collection, retention, and dissemination of information on U.S. citizen employees. A D/A's retention policy must also be reflected in a D/A records schedule approved by the National Archives and Records Administration (NARA).

*All insider threat information for the inquiry that is contained in a system of records that is retrievable by an individual's name or by an identifier associated with a particular individual, is subject to the Privacy Act. D/A must publish in the *Federal Register* notices about the systems of records they maintain (called a System of Records Notice or SORN). The notice must include, among other things, a general description of the type of information contained in the system, the uses of the information, as well as procedures that will permit an individual to request access to information contained in the system. These can be changed through public notice in the *Federal Register.*

*The Federal Records Act requires D/A to retain records in accordance with records control schedules approved for the D/A by NARA. Records can only be retained by a D/A for the period of time specified in the NARA-approved schedule (consultation with the D/A Information Management Office will provide a ready source of advice and expertise). If there is no approved records schedule applicable to a D/A's insider threat program needs, the D/A should initiate action to obtain NARA approval of a records schedule. If a D/A has existing schedules for its records, the D/A can seek NARA approval to adjust the existing schedule to meet insider threat mission needs. The D/A's Information Management Office should be consulted on matters dealing with program records, records retention periods, and records schedules.

--How about retention of records that do not deal with inquiries or investigations? Or information on employees that flows in to the "hub" from other offices but which never becomes part of a D/A inquiry or investigation? What rules should apply to that information?

The same analysis delineated above for records pertaining to inquiries would apply here.

Whistleblowers--

--If an individual within an agency has claimed whistleblower status, is the insider threat program under an obligation to ensure that its computer monitoring no longer covers that employee?

No, as long as the monitoring is done consistently, following the protocols established by the insider threat program for monitoring, then the monitoring need not be terminated because an individual claims whistleblower status. Whistleblower status and computer activity monitoring are both legally-sanctioned activities that, while intersecting, do not interfere with one another.

--Is the D/A under an obligation to identify all its whistleblowers to the insider threat program?

A D/A should not identify its employees who have sought whistleblower status to the insider threat program. Doing so could subject your organization to claims that an individual was being improperly scrutinized because they had made a protected communication.

--Is the D/A under an obligation to develop a technical means to preclude monitoring of all identified whistleblowers?

No, the D/A is under no obligation to develop technical means to preclude monitoring of persons who are identified as whistleblowers.

--If a cleared employee is doing his daily work and decides to go to a website to enter information for a whistleblowing activity, that activity may be captured by insider threat computer monitoring. Isn't this, then, a violation of whistleblower protection afforded to the employee?

No, if a person goes to a website to claim whistleblower status, which is legally sanctioned activity by the person. Likewise, the computer activity monitoring is an equally legal activity. The whistleblower protections protect the individual from retaliation. The conduct of computer monitoring does not constitute retaliation unless there is something showing that the monitoring was conducted as a result of the individual's protected whistleblower status.

Cleared Contractors—

--From a legal and privacy-civil liberties perspective, explain whether the president's policy and minimum standards apply to cleared contractors that are under contract to the federal government.

The National Insider Threat Policy and Minimum Standards are applicable to all employees with access to classified information, including classified computer networks. This includes contractors and others who access classified information or operate or access classified computer networks controlled by the federal government. The definitions of "employee" and "cleared employee" contained in the National Insider Threat Policy and Minimum Standards specifically include an expert or consultant to a D/A, an industrial or commercial contractor, licensee, certificate holder, or grantee of a D/A, including all subcontractors, a personal service contractor, or any other category of person who acts for or on behalf of a D/A, as determined by the appropriate D/A head. D/A should work with your contracting personnel to ensure that your contracts include adequate provisions to implement these requirements.

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

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