

March 3, 2015

MEMORANDUM FOR: Distribution

FROM: Gregory A. Marshall

Senior Insider Threat Official

Chief Security Officer

SUBJECT: Procedures for the Insider Threat Program Concerning Bulk Data Transfers

PURPOSE

The purpose of this memorandum is to provide procedures governing the ingestion of data in bulk for use by the Insider Threat Program (ITP).

BACKGROUND

The ITP is required by Executive Order No. 13,587, “Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information,” October 7, 2011, and the President’s National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs, November 21, 2012, to build and maintain an insider threat analytic and response capability to gather, integrate, review, assess, and respond to information derived from counterintelligence, security, information assurance, human resources, law enforcement, the monitoring of user activity, and other sources as necessary and appropriate. The purpose of these guidelines is to enable the ITP to carry out its authorized functions in an effective manner that also protects the privacy, civil rights, and civil liberties of employees and maintains the integrity of the ITP.

Accordingly, I am issuing the following procedures to establish specific rules governing bulk transfers of data to the ITP. These procedures will provide the ITP with the flexibility it needs to access and maintain information in bulk consistent with the mission requirements of the Department. These procedures are effective as of the signature of this memorandum. The procedures will remain in effect until revoked or otherwise amended.

PROCEDURES

Set forth below are procedures governing all bulk data transfers to the ITP where it is reasonable to believe that the transfer would include significant amounts of Personally Identifiable Information (PII).[[1]](#footnote-1) The term **bulk data transfer** refers to the collection or dissemination of large quantities of intelligence or information, a significant portion of which is not reasonably likely to have any ultimate intelligence or operational value to the recipient, but which is provided to the data recipient for the recipient to identify information of intelligence or operational value within it. Bulk data transfer does not include the transfer of records in response to individual identifiers (e.g., name, date of birth, social security number, etc.), but it does include the transfer of records identified through the application of selectors where the transfer would include a significant number of records that, while responsive to the applied selectors, is not reasonably likely to have any ultimate intelligence or operational value to the recipient (e.g., records responsive to demographic profiles such as age, citizenship, gender, etc.). This policy sets forth two general requirements for bulk data transfers to the ITP.

**Requirement No. 1—Terms and Conditions:** The first requirement for any bulk data transfer to the ITP subject to these procedures is the development of written terms and conditions between the ITP and the data provider governing the ingestion by the ITP.[[2]](#footnote-2) These terms and conditions will be designed to ensure that the transfer is done in a manner that protects individuals’ privacy, civil rights, civil liberties, safeguards information integrity, and accords with applicable law, executive order, presidential and other directive, regulation, international or domestic agreement, arrangement, or obligation, and national and departmental policy. To that end, the written terms and conditions will incorporate the following protections:

* A requirement that any information acquired by the ITP through bulk data transfer will be used only in support of authorized ITP missions and will be transmitted outside the ITP only to the extent permitted by and consistent with the Constitution, executive order, presidential and other directive, regulation, international and domestic agreement, arrangement, or obligation, and national and departmental policy;
* A requirement that any employees or contractors supporting the ITP that are provided access to information acquired via bulk data transfer receive training in the use of that information and understand the baseline and enhanced safeguards, dissemination restrictions, and other privacy expectations and requirements involved in accessing and using such information, including, but not limited to, ongoing training on the requirements set forth by the DHS Chief Privacy Officer, to be taken as a refresher at least once per year, to ensure that such personnel use the information acquired via bulk data transfer only for authorized purposes;
* A requirement that the ITP use reasonable measures to identify and mark (or “tag”) PII concerning United States Persons and any other Special Protected Classes within the data ingested in bulk;
* A requirement that the ITP work with the data provider to ensure that information acquired via bulk data transfer be received, stored, and used in a secure manner consistent with the requirements of the Federal Information Security Management Act, Pub. L. No. 107-347 (2002) (codified at scattered sections of the United States Code), and National Institute for Standards and Technology Special Publication No. 800-53, Recommended Security Controls for Federal Information Systems and Organizations (Aug. 2009), as revised;
* A requirement that, to the extent practicable, data received by the ITP via bulk data transfer be refreshed on a regular, specific schedule reflected in the terms and conditions;
* A specified period during which information acquired via bulk data transfer is permitted to be temporarily retained by the ITP in accordance with written terms and conditions, which will commence when the information is made generally available for access and use following any necessary testing and formatting, and which will not under any circumstances exceed five years in length;
* A requirement that the ITP have methods for updating or correcting errors in the information, purging erroneously provided information, and ensuring continuing data accuracy; and
* Any other safeguards that I, in consultation with the DHS Chief Privacy Officer, the DHS Officer for Civil Rights and Civil Liberties, and the Associate General Counsel for Intelligence, determine are necessary.

**Requirement No. 2—Oversight Office Certifications:** The terms and conditions described above will not go into effect until the following certifications are made:

* From me, a certification that (1) the bulk data to be ingested by the ITP is reasonably likely to contain a significant amount of information that, if acquired by the ITP, would support the identification of insider threats; (2) bulk data transfer is the only practicable means of identifying or using all or a significant amount of the information to be acquired; and (3) that, to the greatest extent practicable, only those data elements within a category of information that are necessary for the lawful conduct of ITP activities are retained by the ITP;
* From the Associate General Counsel for Intelligence, a certification that the terms and conditions are consistent with the requirements of the Constitution, executive order, presidential and other directive, regulation, international and domestic agreement, arrangement, or obligation, and national and departmental policy;
* From the DHS Privacy Officer, a certification that the terms and conditions adequately protect the privacy of any individual whose PII is contained within the bulk data transfer; and
* From the DHS Officer for Civil Rights and Civil Liberties, a certification that the terms and conditions adequately protect the civil rights and civil liberties of any individual whose PII is contained within the bulk data transfer.

In the event that one or more of the other officials named above concludes that a required certificate cannot be issued under the terms and conditions subject to review, I will work with that official (or officials) to resolve any questions or concerns so that appropriate terms and conditions may be memorialized and the bulk data transfer described therein executed. If I cannot resolve any such questions or concerns to the satisfaction of the officials named above and I conclude that the acquisition of data in bulk is appropriate nevertheless, I will refer the matter to the Under Secretary for Intelligence and Analysis so that he or she may work with the Component Head for the office with questions or concerns to resolve the matter. If, following such efforts, required certifications are not forthcoming, the ITP will not execute a bulk data transfer unless the Secretary or Deputy Secretary expressly approve the transfer after appropriate opportunity is provided to the official withholding certification to participate in any discussions with the Secretary or Deputy Secretary leading to that express approval.

**Exception for Exigent Circumstances:** The requirements described above do not apply where the following criteria are met:

* I have determined that a clear, imminent insider threat of such severity exists that the failure to acquire information via immediate bulk data transfer would be reasonably likely to endanger the national or homeland security and the information to be ingested via bulk data transfer relates directly to that insider threat;
* The bulk data transfer is limited to the greatest extent practicable to that necessary to address the insider threat;
* Information transferred via bulk data transfer is afforded the same privacy, civil rights and civil liberties, and information integrity safeguards as information originating within the ITP; and
* Notice of the bulk data transfer under the circumstances described above is provided to the DHS Chief Privacy Officer, the DHS Officer for Civil Rights and Civil Liberties, and the Associate General Counsel for Intelligence as soon as possible, but in no event later than twenty-four hours from the initiation of the bulk data transfer.

*Training and Consultation*

The procedures described above are complex and represent a significant development for the ITP. Accordingly, I direct all ITP employees and contractors to receive training from the Insider Threat Oversight Group on these supplemental policies and procedures within thirty days of assuming the role or responsibilities giving rise to this requirement or ninety days of the execution of these procedures, whichever occurs last, and once per year thereafter. In addition, such personnel will consult with the Insider Threat Oversight Group prior to developing or implementing any automated information system to be maintained by the ITP that is reasonably likely to contain significant amounts of PII concerning United States Persons.

CONCLUSION

These procedures apply to all ITP employees (including assignees, detailees, and persons acting for the ITP) and contractors supporting the ITP that provide support to bulk data transfers or the hosting of shared repositories by the ITP. They do not substitute for legal review of specific information sharing activities, and any questions concerning the applicability or interpretation of these procedures should be referred to the Associate General Counsel for Intelligence.

These procedures are set forth solely for the purpose of internal ITP guidance. They do not create any substantive or procedural rights enforceable by law or by any other party in a civil or criminal matter, nor do they place any limitation on otherwise lawful investigative and litigation prerogatives of the United States Government.

Distribution:

Chip Fulghum, Acting Deputy Under Secretary for Management

Francis X. Taylor, Under Secretary for Intelligence and Analysis

Karen Neuman, Chief Privacy Officer

Megan Mack, Officer for Civil Rights and Civil Liberties

Stevan Bunnell, General Counsel

Matthew L. Kronisch, Associate General Counsel for Intelligence

1. PII refers to any information that permits the identity of an individual to be directly or indirectly inferred, including any other information that is linked or linkable to that individual. This definition applies regardless of whether the individual is a United States citizen, lawful permanent resident, visitor to the United States, DHS employee, or contractor. [↑](#footnote-ref-1)
2. It may not always be possible to enter into a formal written terms and conditions with a data provider. For example, the terms and conditions of a contract with a vendor providing publicly available commercial information would not incorporate all of the terms and conditions required by this policy, or a foreign partner may not be able to enter into a formal agreement for political reasons. Where entry into a formal agreement is impermissible or impracticable, the ITP may satisfy the requirement for written terms and conditions through the development of an internal document provided that (1) a copy of this internal document is shared with the data provider, as appropriate, and (2) all other requirements of this policy are satisfied, including the need for certifications from myself, the Associate General Counsel for Intelligence, the DHS Chief Privacy Officer, and the DHS Officer for Civil Rights and Civil Liberties. [↑](#footnote-ref-2)