The National Counterterrorism Center

Overview of the Baseline Safeguard Protections Under NCTC's 2012 Attorney General Guidelines

Background

The National Counterterrorism Center (NCTC) is "the primary organization in the United States Government for analyzing and integrating all intelligence possessed or acquired by the United States Government pertaining to terrorism and counterterrorism" (National Security Act of 1947, as amended). In order to perform this statutory mission, NCTC, like other intelligence community elements, is required by law and Executive Order to have guidelines approved by the Attorney General and the Director of National Intelligence (DNI) relating to its handling of information about United States persons.[1]

In the aftermath of the December 25, 2009 attempted terrorist attack against a Detroit-bound flight, NCTC recognized that it needed to retain replicated datasets[2] for longer periods[3] to identify previously unknown relationships to terrorism information, which might become evident only after time-consuming correlation with other datasets, or with the discovery of new information at later points in time. Consequently, in March 2012, the Attorney General, DNI, and Director of NCTC signed updated *Guidelines for Access, Retention, Use, and Dissemination by the National Counterterrorism Center and Other Agencies of Information in Datasets Containing Non-Terrorism Information* (frequently referred to as NCTC's 2012 Attorney General Guidelines)[4]. These Guidelines are critical to helping NCTC carry out its mission under the National Security Act of 1947, while protecting information about United States persons.

The primary change under the revised Guidelines was to extend the length of time that NCTC may temporarily retain and assess replicated datasets for a nexus to terrorism—also referred to as Track 3 data[5]—after which all U.S. person information not "reasonably believed to constitute terrorism information" must be purged from NCTC's systems. In order to protect the privacy and civil liberties of individuals during this temporary retention period, the revised Guidelines also implement a series of civil liberty and privacy protective measures, including baseline safeguards (to be applied to all datasets being temporarily assessed by NCTC), enhanced safeguards (which are dataset specific, and are designed to address unique sensitivities that may apply in individual datasets, requiring additional protections over and above the baseline safeguards)[6], as well as audits, oversight and reporting requirements.

Baseline Safeguards Required Under the 2012 Guidelines

One of the important protections that NCTC applies to all datasets replicated and assessed at NCTC under the 2012 Guidelines is the application of baseline safeguards.[7] Notably, baseline safeguards are applied by NCTC to all datasets at the time of replication, regardless of the data provider, the specific type of data, or whether the data provider affirmatively requested such safeguards.[8]

- **Baseline Safeguard 1:** "[D]atasets will be maintained in a secure, restricted-access repository";
- **Baseline Safeguard 2:** "Access to these datasets will be limited to those NCTC personnel who are acting under, and agree to abide by, NCTC's information sharing and use rules, including these Guidelines; who have the requisite security clearance and a need-to-know in the course of their official duties; and who have received the training required";

[1] As defined in Executive Order 12333, a United States person means "a United States citizen, an alien known by the intelligence element concerned to be a permanent resident alien, an unincorporated association substantially composed of United States citizens or permanent resident aliens, or a corporation incorporated in the United States, except for a corporation directed and controlled by a foreign government or governments."

[2] For additional information on the pre-requisites for NCTC's replication of data, and the categories of data replicated by NCTC from other federal agencies, please see NCTC's *Overview of NCTC's Data Access as Authorized by the 2012 Attorney General Guidelines,* available at *www.nctc.gov.*

[3] For additional detail on how these events tied into the need for revision of NCTC's Attorney General Guidelines, please see NCTC's *Mission Justification Fact Sheet*, available at *www.nctc.gov.*

[4] Available at *www.nctc.gov.*

[5] Under NCTC's revised Guidelines, NCTC uses three *tracks* to access or acquire federal datasets. Under *Track 1*, NCTC analysts are given account-based access to a relevant federal agency dataset, while under *Track 2*, NCTC provides its query terms to a federal agency for that federal agency to perform the search and return responsive information. With *Track 3*, a federal agency dataset is replicated (in whole or in part) into NCTC's systems so that NCTC can use its analytic tools to assess the data within the dataset in order to identify terrorism information.

[6] Because enhanced safeguards are assessed and applied on a dataset by dataset basis, implementation of the spot checks and audits of enhanced safeguards is likewise performed on an individualized basis. For more information on the factors that NCTC considers in assessing a dataset for enhanced safeguards, and the types of safeguards potentially applied, please see NCTC's *Enhanced Safeguards Decision Matrix*, available at *www.nctc.gov.*

[7] Section III.C.3(d) of the Guidelines.

[8] Notably, although the 2012 Guidelines were designed specifically to protect United States persons, the protections in these Guidelines are often also applied to non-United States persons information (as contained in Track 3 datasets), to include application of the baseline safeguards (as well as the audits and spot checks of those safeguards).

Baseline Safeguards Required Under the 2012 Guidelines —continued

- **Baseline Safeguard 3:** "Access to these datasets will be monitored, recorded, and audited. This includes tracking of logons and logoffs, file and object manipulation and changes, and queries executed, in accordance with audit and monitoring standards applicable to the Intelligence Community. Audit records will be protected against unauthorized access, modifications, and deletion, and will be retained for a sufficient period to enable verification of compliance with rules applicable to the data for which audit records apply."
- **Baseline Safeguard 4:** "NCTC's queries or other activities to assess information contained in datasets acquired pursuant to Track 3 shall be designed solely to identify information that is reasonably believed to constitute terrorism information. NCTC shall query the data in a way designed to minimize the review of information concerning United States persons that does not constitute terrorism information."
- **Baseline Safeguard 5:** "NCTC will conduct compliance reviews," which shall "include spot checks, reviews of audit logs, and other appropriate measures."

Implementation and Compliance Audit of the Baseline Safeguards (as of February 2014)[9]

Baseline Safeguard 1	
Requirement	Datasets maintained in a secure, restricted-access repository.
Implementation	For this baseline safeguard NCTC focuses on *privileged users*[10] who have system administrator-like access to the secure, restricted access repositories where all replicated datasets are maintained. In addition to training these privileged users on appropriate access to, and use of, these datasets, NCTC audits these repositories on a regular basis.
Compliance Audit Process	NCTC will conduct random spot checks of accesses to all servers that host Track 3 data to verify that only approved privileged users had access to these repositories, and that those users only accessed datasets for which they were authorized. To do this, a script will randomly select a reasonably significant number of servers from all of the servers hosting Track 3 data[11] over a specified time period. A script will then be run to randomly select a predetermined number of logons to the servers selected for review. NCTC managers will then conduct a detailed evaluation of this pre-determined number of randomly selected logons within that time frame in order to validate that only authorized users gained access and that those users were acting in accordance with their authorized roles at the time of access. If any unauthorized accesses are identified, they will be forwarded to the NCTC Compliance Team for further review and action.
Baseline Safeguard 2	
Requirement	Access to datasets limited to NCTC personnel who: a) are acting under, and agree to abide by, NCTC's information sharing and use rules; b) have the requisite security clearance and a need-to-know in the course of their official duties; and c) who have received the training required for such.

[9] This "as of date" is important to note, because implementation of the baseline safeguards at NCTC is still in its early stages, and NCTC expects to continue to modify, refine and revisit these baseline safeguard processes over time.

[10] A privileged user is one who, by virtue of function, has been allocated permissions within the computer system, which are significantly greater than those available to the majority of users. Such persons will include, for example, System Administrators, Network Administrators, and Database Administrators, each of whom is responsible for keeping the system available, and may therefore need permissions to maintain server performance and data integrity.

[11] As a general rule, a server can host multiple Track 3 datasets. Likewise, a Track 3 dataset can reside on more than one server (i.e., dataset A—a Track 3 dataset—could theoretically be hosted on five separate servers).

—continued

Implementation and Compliance Audit of the Baseline Safeguards (as of February 2014)

Implementation	Baseline Safeguard 2 is implemented through NCTC's role-based access policy, and focuses on *non-privileged users*.[12] More specifically, role-based access to datasets within NCTC is restricted by membership in pre-approved virtual groups (generally, broken out by offices within an individual NCTC Directorate); each of these pre-approved virtual groups is administered by a lead in charge of maintaining the group (generally, a manager from the office that corresponds to the group membership) (hereafter "virtual group administrator"). When an employee physically moves to a new office within NCTC, that employee's accesses to datasets are reassessed and updated (as needed), based upon mission need within the new assignment. In order to join one of these groups—and thereby gain access to data—NCTC first verifies that the employee has agreed to adhere to NCTC's information sharing and use rules, holds the appropriate security clearance, has a need to know in the course of official duties, and has completed all of the requisite training necessary to access a given dataset. In addition, to remain a member of these virtual groups, employees must also undertake annual training on data access and use, privacy, and handling of U.S. person information, which details the obligations and protections under our Attorney General Guidelines. Failure to complete annual training results in loss of access to the data, as well as a potential negative rating on the employee's annual performance evaluation.
Compliance Audit Process	NCTC will conduct spot checks of each of these pre-approved virtual groups to ensure that the membership is accurate and up to date (and therefore, that continued access by all members of the group to that particular dataset is appropriate). Specifically, NCTC will randomly choose an audit date, and then notify each of the virtual group administrators of this audit. These virtual group administrators will then compare the pre-approved group member list generated on the day of the audit against an up to date office staffing list for that same date. If all members of the pre-approved group are still employed in the corresponding office group on the chosen date, and have a continued need to access that dataset, then the administrator will have verified role-based access for that group. If, on the other hand, an individual listed in the pre-approved group no longer has a need to access the dataset—for example, because that employee has since left the office, or moved to a new group—then the administrator will further check to see: 1) whether the individual in question actually gained access to a dataset using the outdated group membership during the period of time when the individual should not have had access; and 2) if an actual access was identified, whether the employee was authorized to access that dataset in his/her new role (i.e., if the employee's new group is also authorized to access the same dataset, then there has been no unauthorized access to the dataset, even though the previous group's membership list will need to be updated). If an unauthorized access is identified during this review, the incident is forwarded to the NCTC Compliance Team for further action.

[12] A non-privileged user is an ordinary user, with limited access to search and review data, and who does not have the ability to change or manipulate that data, nor to access areas reserved for those with system administrator privileges (i.e., privileged users).

—continued

Implementation and Compliance Audit of the Baseline Safeguards (as of February 2014)

Baseline Safeguard 3	
Requirement	Access to datasets will be monitored, recorded, and audited, to include tracking of logons and logoffs, file and object manipulation and changes, and queries executed. Audit records will be protected against unauthorized access, modifications, and deletion, and will be retained for a sufficient period to enable verification of compliance.
Tracking Log-ons and Log-offs	
Implementation	For this baseline safeguard NCTC focuses on *non-privileged users*.[13] Once an employee logs on to the system, there is no independent logon to a dataset. As such, NCTC defines "logons" as any access/query of a dataset via an application accessible to an NCTC user (such as the use of NCTC's internal, Google-like search engine). The ending of a query or set of queries on a dataset will constitute a "logoff" from the dataset for purposes of this spot check. Notably, this spot check provides a counter-check of the role-based access check conducted for Baseline Safeguard 2. In other words, if an individual is able to access a dataset, even when s/he was not on the access list for that dataset (as verified under Baseline Safeguard 2), this will highlight the existence of a technical issue that needs to be addressed.
Compliance Audit Process	NCTC will pull all queries entered against Track 3 datasets over a pre-determined period of time (each query constituting a logon to the dataset). NCTC will also pull the relevant information associated with each access/logon, to include the name of the individual running the query and the name of the particular Track 3 dataset searched. A script will then be run to compare the list of datasets that each user queried, against their authorized organization, user roles, and clearances to validate that the person had the proper role, assignment, credentials, and need for access to each dataset. If all individual accesses to a dataset are found to be authorized, then no additional action is taken and these logons will have been verified as appropriate. If any individual is identified as having accessed (i.e., logged on) to a dataset despite his/her name not having been on the approved access list for that dataset (i.e., the individual was not a member of one of the virtual groups approved for accessing this dataset, as validated under Baseline Safeguard 2), the name of that individual (and the datasets accessed) is forwarded to a supervisor for further review. In conducting this review, the supervisor will assess whether that individual had reason and authorization to access the dataset (in which case the individual's role based access credentials need to be updated). Supervisors will also work with Mission Systems to determine how the logon occurred given the absence of that person's name on the access list, in order to identify and fix any potential technical problems that may not have previously been identified. Logons to a dataset will be presumed appropriate and authorized if the supervisor verifies the user's role and need to access the dataset in the course of his/her expected duties on the date of the spot check. If, on

[13] A user may hold roles as both a privileged and non-privileged user, depending upon how they are accessing data. Any time a dataset is accessed via an application (without the use of special system administrator privileges), the user is deemed a non-privileged user.

—continued

Implementation and Compliance Audit of the Baseline Safeguards (as of February 2014)

	the other hand, it's determined that the individual did not have a need/role to access the dataset, then the supervisor will further work with Mission Systems (MS) to determine how the logon to the Track 3 dataset occurred and how to eliminate such logons in the future. This incident will also be reported to the NCTC Compliance Team for further review.
Tracking of File and Object Manipulation and Changes	
Implementation	For this baseline safeguard NCTC focuses on privileged users because file/object changes and manipulations can only be made by privileged users. While non-privileged users can search and view data, they cannot change the data (i.e., they have no write access).
Compliance Audit Process	A script will randomly select a reasonably significant number of servers from all of the servers hosting Track 3 data over a predetermined period of time. A script is then run to randomly select for review a predetermined number of changes/manipulations made to Track 3 data for each of the chosen servers. In order to prioritize the review of changes/manipulations made by humans/privileged users—the primary focus of this spot check—to the extent practical the script will be updated over time to differentiate between automated machine changes (e.g., when data is updated by a provider, via automatic process), and human/privileged user made changes. All of the selected changes/manipulations per server identified as having been made by a human/privileged user are then forwarded to the government lead that oversees the selected server, to assess the propriety of each change/manipulation flagged. If any unauthorized changes/manipulations are identified by the government lead, a description of the unauthorized change/manipulation will be provided to MS to conduct a review—in conjunction with the NCTC Compliance Team—to identify remedial measures and amend/correct accordingly.
Tracking of Queries Executed	
Queries executed will be monitored, recorded, and audited using NCTC's procedures implementing Baseline Safeguard 4, described below.	
Protection and Verification of Audit Records	
Implementation	For this Baseline Safeguard NCTC focuses on privileged users, reviewing audit records to ensure that these records have not been tampered with (i.e., to verify and document that there were no unauthorized accesses, modifications, or deletions made to those audit records). Audit records are defined as a detailed recording or logging of all system activity and events involving access to and/or modification of Track 3 data. Audit records are captured for every activity relating to NCTC's handling of data, including all activities which are subject to compliance monitoring under each of the four Baseline Safeguards (e.g., accesses, queries, changes/manipulations, etc.). Because it's possible for audit records to be changed or deleted by privileged users, NCTC also maintains a separate audit log of all actions taken with regard to the audit records (i.e., an audit of the audit log). This audit log cannot be changed, even by a privileged user, and is therefore referred to as an "immutable audit log". All audit records and the immutable audit log will be retained for no

—continued

Implementation and Compliance Audit of the Baseline Safeguards (as of February 2014)

	less than 5 years, in accordance with the Federal Records Act, NCTC's applicable records control schedules, and Intelligence Community Standards.
Compliance Audit Process	NCTC analyzes entries in the immutable audit log (which tracks all actions taken with regard to the audit records) for a pre-determined period of time (that period of time being randomly chosen by NCTC), in order to identify any attempted or actual changes to the audit records during that period. Any actual or attempted changes to the audit records—as identified through a comparison of the audit records against the immutable audit log—will then be forwarded for further evaluation to the government lead responsible for maintaining these audit records. As a general rule, there should never be changes or deletions to audit records other than those made for authorized maintenance purposes (e.g., audit records may be deleted by a privileged user to free additional storage space). It is therefore the government lead's responsibility to distinguish between authorized and unauthorized changes to the audit records. If unauthorized changes to audit records are identified, the matter is then forwarded to the NCTC Compliance Team for further review, and the original record (that was changed without authorization) is then corrected using a back-up copy of the same audit record.[14]
Baseline Safeguard 4	
Requirement	Queries or other activities to assess information contained in datasets acquired pursuant to Track 3 shall be designed solely to identify information reasonably believed to constitute terrorism information. NCTC shall query the data in a way designed to minimize the review of information concerning United States persons that does not constitute terrorism information.
Implementation	To ensure that queries against Track 3 datasets are narrowly tailored in accordance with the query design requirements of the 2012 NCTC Attorney General Guidelines, query reviews will be periodically conducted by Branch Chiefs from all branches that use Track 3 data. Prior to conducting query reviews, Branch Chiefs will first attend mandatory Branch Chief Query Review Training to ensure both a clear understanding of the 2012 NCTC Attorney General Guidelines and the resultant requirements set forth in those Guidelines with regard to proper querying of Track 3 data.
Compliance Audit Process	Once the designated timeframe within the respective audit period has been chosen, NCTC will implement a process where all queries run on Track 3 datasets during the specified time period are, for each respective branch, randomized and populated into a user interface for review. A predetermined number of randomly selected queries will then be produced for each branch to review. The number of queries produced for review in any given period may change based upon lessons learned from one audit to the next. To facilitate and automate the query review process, NCTC has created a SharePoint site to serve as a user interface. The SharePoint will be populated with each Branch's randomly selected queries. The Branch Chief Query Review Training will include a demonstration of the SharePoint site as the Branch Chief will both

[14] As an additional protection, audit records are also backed up to a second location immediately after they are created.

—continued

Implementation and Compliance Audit of the Baseline Safeguards (as of February 2014)	review and adjudicate the query within the SharePoint. Each query reviewed will then be assessed by the Branch Chief to ensure that the query is designed solely to identify information that is reasonably believed to constitute terrorism information while minimizing the review of information concerning US persons that does not constitute terrorism information. All non-compliant queries will be reported to the NCTC Compliance Team. As an additional protection, Branch Chiefs will not be permitted to review their own queries. Should a Branch Chief's query come up for review, a process has been implemented to ensure that this Branch Chief's query is reviewed by another Branch Chief for purposes of compliance validation.

Oversight of NCTC's Compliance

The NCTC Civil Liberties and Privacy Officer (NCTC CLPO) and the NCTC Office of Legal Counsel will provide oversight of NCTC's compliance with all of these safeguards, spot checks and other audit mechanisms, to include reviewing the results of the spot checks and audits conducted by NCTC for Baseline Safeguards 1-4.

Any compliance incidents identified through the above spot checks is forwarded to the NCTC Compliance Team for a compliance review, conducted using NCTC's compliance incident review process, in accordance with NCTC's *Compliance Incident Procedures Regarding Data Handling.*[15]

As required by the 2012 Attorney General Guidelines, NCTC will also notify the Department of Justice and the IC Inspector General (as well as all other appropriate oversight entities, such as the President's Intelligence Oversight Board) upon discovery of an incident that constitutes a "significant failure" to comply with the Guidelines, the Safeguards, and/or any Terms and Conditions documents. Likewise, NCTC will continue to keep its Congressional oversight committees fully and currently informed of any such compliance incidents.

Ongoing Compliance and Auditing Enhancements

Because implementation of the Baseline Safeguards at NCTC is still in its early stages, NCTC expects to continue to modify, refine and revisit these Baseline Safeguard processes over time, as experiential data is gathered and results of the spot checks and audits are checked against the original intent of the process in question.

Likewise, pursuant to Section VI.C of NCTC's 2012 Attorney General Guidelines, in designing its computer systems NCTC has a continuing obligation to "take reasonable steps to enhance its ability…to facilitate compliance with, and auditing and reporting" required by the Guidelines. As such, NCTC expects that this document will continue to evolve, and improve, over time, as NCTC continues to look for new ways to protect both the data with which it has been entrusted, and the privacy rights of individuals whose information is contained within that data.

[15]Available at *www.nctc.gov*.