Privacy Impact Assessment
for the

DHS Management Cube

DHS/ALL/PIA-081

January 30, 2020

Contact Point
Robert C. King
Director, Systems and Information Integration Office
Office of the Chief Readiness Support Officer
Department of Homeland Security
(202) 536-9955

Reviewing Official
Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The Department of Homeland Security's (DHS) Management Cube (MGMT Cube) is a business intelligence tool owned by the DHS Management Directorate. MGMT Cube houses financial, acquisition, human resources, contracting, asset, and security data about DHS and its personnel for executive management analysis and decision making. This Privacy Impact Assessment (PIA) is being conducted as MGMT Cube uses personally identifiable information (PII) from personnel across the DHS enterprise.

Overview

MGMT Cube is an information technology application developed by the DHS Management Directorate (Management) to evaluate functions across Management's Chief Executive Offices (CXO).[1] MGMT Cube does not collect information directly from individuals, but rather aggregates data from Management's source systems to create analytic reports on DHS personnel, assets, financials, and budgeting. Specifically, the application aggregates data on financial, acquisition, human resources, contracting, asset, and security information from each CXO to facilitate management analysis and decision making. MGMT Cube, in part, aggregates the supplied data from Management systems to create analytic reports on DHS employees and contractors, such as demographic data, calculations of retirement eligibility, and other macro-level data analyses. Authorized users may access this data to answer Department-wide business questions about DHS's workforce, funding, and investments.[2] Centralizing information across the CXOs permits the Department to establish trends, improve data quality, eliminate duplicative data calls, and improve collaboration among officials in finance, procurement, human resources, information technology, physical security, and other management functions.

Only two Management systems providing data to MGMT Cube contain personally identifiable information (PII):

1) The Human Capital Business Systems Enterprise Integration Environment (HCBS EIE), owned by the DHS Office of the Chief Human Capital Officer (OCHCO); and

2) The Integrated Security Management System (ISMS),[3] owned by the DHS Office of the Chief Security Officer (OCSO).

---

[1] DHS CXOs, for purposes of the DHS Management Cube, include the Office of the Chief Financial Officer (OCFO), the Office of the Chief Human Capital Officer (OCHCO), the Office of the Chief Information Officer (OCIO) the Office of the Chief Procurement Officer (OCPO), the Office of the Chief Readiness Support Officer (OCRSO), the Office of the Chief Security Officer (OCSO), and the Office of Program Accountability and Risk Management (PARM).

[2] "Investment" is defined in the DHS lexicon as a "resource committed to achieve specific goals and objectives." Examples of investments include people, assets, equipment, services, supplies, and systems.

[3] *See* DHS/ALL/PIA-038 Integrated Security Management System (ISMS), *available at* https://www.dhs.gov.privacy.

The type of data MGMT Cube pulls from other CXOs includes:

- OCFO: programming and budgeting data;
- OCIO: enterprise architecture, investment, and acquisitions data;
- OCPO: post-award contract data;
- OCRSO: aggregated real and personal property data; and
- PARM: acquisition data from programs on the DHS's Master Acquisition Oversight List.

Human Capital Business Systems Enterprise Integration Environment (HCBS EIE)

HCBS EIE is OCHCO's authoritative human resources system that provides personnel data feeds of DHS employees to support DHS-wide human resource systems and applications. The National Finance Center Payroll/Personnel System (NFC PPS)[4] delivers most of the information on an automated biweekly basis to HCBS EIE, which then provides a subset of DHS employee data to MGMT Cube. Importantly, prior to importing the employee data to MGMT Cube, HCBS EIE filters out sensitive personally identifiable information (*e.g.*, Social Security numbers (SSN), financial account numbers). In order to protect the PII contained in this system, ISMS generates and associates a unique personal identifier for every DHS employee, or "person handle," to every record in the system relating to individuals within HCBS EIE. The person handle consists of a 10-digit number that is uniquely and directly attributable to each record containing personal information. As such, the person handle is the attribute that MGMT Cube system administrators and data migration automation use to align the two data sets together.

The OCHCO human resources data analytics team receives data from the NFC and migrates it into HCBS EIE. Once in HCBS EIE, a subset of the original NFC data is copied to MGMT Cube via data migration automation. The personnel data is managed in two categories: 1) data elements available only to MGMT Cube system administrators for data alignment; and 2) data elements that are aggregated for creating analytic reports in MGMT Cube.

Integrated Security Management System (ISMS)

ISMS is a DHS-wide web-based case management application designed and managed by OCSO, which is under the Management Directorate. ISMS supports the lifecycle of DHS personnel security, administrative security, and classified visitor management functions. The system manages, in part, data related to suitability determinations, background investigations, and security clearance processing. PII maintained in ISMS consists of employee SSN and other

[4] The National Finance Center Payroll/Personnel System is a system managed by the U.S. Department of Agriculture (USDA) to facilitate personnel and payroll functions for more than 130 federal organizations, including DHS. *See* Privacy Impact Assessment – National Finance Center Payroll/Personnel System, *available at* https://www.usda.gov/home/privacy-policy/privacy-impact-assessments.

identifying information required to perform and track background investigations and to coordinate other security-related processes related to DHS personnel.[5]

In order to protect the PII contained in this system, ISMS generates a personal identifier, or "person handle," for every record in the system relating to individuals. The person handle consists of a 10-digit number that is uniquely and directly attributable to each record containing personal information. ISMS uses the person handle as a primary key to manage other data associated to the record. In order to minimize privacy risks, the person handle is used, instead of SSNs and other unique identifiers, for personnel identification and tracking purposes within MGMT Cube.

MGMT Cube extracts data elements from ISMS on a weekly basis, which are managed in two categories: 1) data elements available only to MGMT Cube system administrators for data alignment; and 2) data elements that will be aggregated for creating analytic reports in MGMT Cube.

The individual source system owners and the system owner of MGMT Cube each sign a Memorandum of Understanding designating a representative to facilitate MGMT Cube authorizations and initiatives. One of the functions each representative performs is to review all reports and dashboards to ensure information is appropriately aggregated, so individuals cannot be identified by the content displayed in MGMT Cube. All authorized users must also review and sign a Rules of Behavior for MGMT Cube *(MGMT Cube Rules of Behavior),* which in part acknowledges that they will be held accountable for actions while accessing and using MGMT Cube. Authorized users also receive training on MGMT Cube.

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

In addition to the authorities listed in the source system SORNs in Section 1.2, the below are specific authorities or agreements that permit the collection of information and define MGMT Cube requirements.

DHS Delegation 00002, *Delegation to the Under Secretary for Management* (revised April 13, 2018) – the Under Secretary for Management oversees the transformation process by establishing unified policies and business processes, the use of shared or centralized services and standards, and automated solutions, for the purpose of achieving excellence in support of the Department's missions and objectives.

[5] For a thorough examination of PII data elements maintained in ISMS, *see* DHS/ALL/PIA-038 Integrated Security Management System (ISMS), *available at* https://www.dhs.gov/privacy.

DHS Management Directive 142-02, *Information Technology Integration and Management* (April 12, 2018) – establishes the DHS's authorities, responsibilities, and policies of the DHS Chief Information Officer and Components' Chief Information Officers regarding information technology integration and management.[6]

DHS Management Directive 103-01, Enterprise Data Management Policy (August 25, 2014) – outlines policy on the management of Enterprise Data, data that is created, managed, or maintained within DHS that is common to, or shared among, multiple DHS entities.[7]

Pub. L. 106-554, Treasury and General Government Appropriations Act for Fiscal Year 2001 (February 22, 2002) - directs the Office of Management and Budget (OMB) to issue government-wide guidelines that provide policy and procedural guidance to federal agencies for ensuring and maximizing the quality, objectivity, utility, and integrity of information (including statistical information) used by federal agencies.

Office of Management and Budget, *Guidelines for Ensuring and Maximizing the Quality, Objectivity, Utility, and Integrity of Information Disseminated by Federal Agencies* (September 28, 2001) – which outlines the government-wide guidelines provided by OMB fulfilling the requirements of Treasury and General Government Appropriations Act for Fiscal Year 2001.

DHS Under Secretary for Management, *Dashboard Executive Steering Committee Charter* (May 2, 2012) – establishes an executive body to provide strategic direction for integrating existing business intelligence and dashboard capabilities across DHS's Management directorate.

1.2 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

ISMS records are covered by the following SORNs:

- DHS/ALL-023 Personnel Security Management System of Records;[8] and
- DHS/ALL-024 Facility and Perimeter Access Control and Visitor Management System of Records.[9]

HCBS EIE is a system from which all human resources-related information about individuals within MGMT Cube is derived. HCBS EIE records are covered by the following SORNs:

[6] *See* https://www.dhs.gov/sites/default/files/publications/mgmt/information-and-technology-management/mgmt-dir_142-02-info-tech-integration-and-mgmt_revision-01.pdf.
[7] *See* https://www.dhs.gov/sites/default/files/publications/08.%20Directive%20103-01%20Enterprise%20Data%20Management%20SIGNED%2008-25-2014_0.pdf.
[8] DHS/ALL-023 Personnel Security Management System of Records, 75 FR 8088 (February 23, 2010).
[9] DHS/ALL-024 Facility and Perimeter Access Control and Visitor Management System of Records, 75 FR 5609 (February 3, 2010).

- OPM/GOVT-1 General Personnel Records;[10]
- OPM/GOVT-2 Employee Performance File System Records;[11]
- DHS/ALL-003 Department of Homeland Security General Training Records;[12] and
- DHS/ALL-019 Payroll, Personnel, and Time and Attendance Records System of Records.[13]

1.3 Has a system security plan been completed for the information system(s) supporting the project?

MGMT Cube resides on DHS's Business Intelligence as a Service (BIaaS) platform. BIaaS manages the servers, services, and system access controls for MGMT Cube. As such, MGMT Cube adheres to all of the security controls in the BIaaS system security plan. The BIaaS system is operating under a valid Authority to Operate until November 2020; a new system security plan is currently in development.

1.4 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

Yes. Reports created by MGMT Cube are covered by NARA General Records Schedule (GRS) 5.2, item 020, *Intermediary Records*. Records from HCBS EIE, ISMS, and other source systems will be maintained in accordance with the source system retention requirements.

1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

MGMT Cube information is not covered by the PRA because information is collected from DHS personnel and not from members of the public.

[10] OPM/GOVT-1 General Personnel Records, 77 FR 73694 (December 11, 2012).
[11] OPM/GOVT-2 Employee Performance File System Records, 71 FR 35342 (June 19, 2006).
[12] DHS/ALL-003 Department of Homeland Security General Training Records, 73 FR 71656 (November 25, 2008).
[13] DHS/ALL-019 Payroll, Personnel, and Time and Attendance Records System of Records, 80 FR 58283 (September 28, 2015).

Section 2.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected, as well as reasons for its collection.

2.1 Identify the information the project collects, uses, disseminates, or maintains.

MGMT Cube contains data from the Management CXOs, which include the Office of the Chief Financial Officer (OCFO), the Office of the Chief Human Capital Officer (OCHCO), the Office of the Chief Information Officer (OCIO), the Office of the Chief Procurement Officer (OCPO), the Office of the Chief Security Officer (OCSO), the Office of the Chief Readiness Support Officer (OCSRO), and the Office of Program Accountability and Risk Management (PARM). Specifically, the PII elements contained in MGMT Cube are outlined below.

HCBS EIE data elements available only to MGMT Cube system administrators:

- Person handle (unique identifier for an individual used in lieu of Social Security numbers (SSN) to align data sets together);
- Date of birth (DOB) (for average age and retirement calculations);
- Master record number (unique number assigned to general position categories);
- Individual position number (links to the master record and identifies a specific position, but not an individual); and
- Physical disability code and description.

HCBS EIE reportable data elements available in aggregated analytic reports in MGMT Cube:

- Duty station city, county, state, country, and codes (designates location where individual is employed);
- Location, component, and organization name and codes (DHS office where individual is employed);
- Job series and code (designates individual's federal job category);
- Position title;
- Age;
- Length of service (length of time employee has worked for the U.S. Government);
- Service computation date for leave and retirement (dates at which employee is considered to have begun federal employment for purposes of computing annual leave and retirement);
- Law enforcement officer indicator (indicates whether employee is a law enforcement officer);
- Retirement indicator (indicates employee's retirement status);

- Supervisory code (designates whether employee is a supervisor);
- Pay plan (defines the federal civilian pay system that covers the individual);
- Veteran preference status and code (identifies whether employee is entitled to a preference in federal hiring based on military service, and if so, the type of preference granted);
- Ethnicity;
- Gender (federal employee only);
- Department code (indicates the DHS component where the individual is employed);
- Personnel office identifier (office authorized to conduct human resources functions on behalf of employee);
- Grade (the pay level for General Schedule and Wage Grade employees);
- Pay period begin and end date (date range of employee's current pay period); and
- Pay period year and number (specific pay period within annual pay cycle).

ISMS data elements available only to MGMT Cube system administrators:

- Position handle (a string of 17 characters uniquely identifying an employee's position, the first 10 of which represent the employee's person handle);
- Electronic Data Interchange Personal Identifier (EDIPI) (a unique 10-digit number associated with an employee's personal identity verification (PIV) card);[14]
- Last investigation type and date (scope and level of clearance investigation conducted and date clearance was granted);
- DOB (contractor only);
- Processing start date (date personnel security began processing clearance);
- Initial determination date and decision (date personnel security rendered an initial suitability determination and result of decision);
- Final determination date and decision (date personnel security rendered a final suitability determination and result of decision); and
- Actionable decision date (date at which employee received a favorable suitability determination).

ISMS data elements that will be aggregated for creating analytic reports in MGMT Cube:

- Organization levels 1 and 2 (identifies the employee's organization down to the DHS Component level);
- Organization (represents lowest level in organization hierarchy to which employee is assigned);

[14] For information regarding privacy implications related to PIV card issuance and management, *see* DHS/ALL/PIA-014 Personal Identity Verification/Identity Management System (PIV/IDMS), *available at* https://www.dhs.gov/privacy.

- Employee group and type (employee's DHS subcomponent and whether the employee is federal, contractor, or military);
- Clearance level (suitability, confidential, Secret, or Top Secret);
- Date clearance granted;
- Duty location city, state, and country and code;
- Contractor company name and contract number (if applicable);
- Contractor primary position (contractor position description, if applicable);
- Contractor position status (whether contactor is currently active on contract, if applicable);
- Date position created (contractor only);
- Date employee status changed (date last position description changed for a contractor, if applicable);
- Position separation date (date contractor left position, if applicable);
- Position title (contractor only); and
- Gender (contractor only).

2.2 What are the sources of the information and how is the information collected for the project?

The only Management systems populating MGMT Cube with PII are:

- Office of the Chief Human Capital Officer's *Human Capital Business Systems Enterprise Integration Environment* (HCBS EIE) system; and
- Office of the Chief Security Officer's *Integrated Security Management System* (ISMS).

MGMT Cube automatically extracts data from HCBS EIE on a biweekly basis and from ISMS on a weekly basis.

2.3 Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

No. MGMT Cube does not use publicly available data about individuals.

2.4 Discuss how accuracy of the data is ensured.

Each CXO data source owner conducts its own data accuracy assessments prior to MGMT Cube ingesting its data. MGMT Cube automatically ingests the data without alteration. The system then employs automated quality controls that identify inconsistencies among similar data sets to ensure data integrity and quality. MGMT Cube provides traceability back to the CXO data sources for all data elements collected, so any inaccurate data is identified and reported to the appropriate CXO system owner for correction.

2.5 Privacy Impact Analysis: Related to Characterization of the Information.

Privacy Risk: There is a risk that MGMT Cube users may be able to access information about individuals in MGMT Cube without a need-to-know.

Mitigation: This risk is partially mitigated. MGMT Cube contains specific security controls that require database accounts in order to access the system on a need-to-know basis. Prior to gaining access to MGMT Cube, approvals must be obtained by the system owner, system administrators, and the Information System Security Officer (ISSO). MGMT Cube does not independently manage access to the servers, but rather uses DHS HQ data center security practices outlined in DHS 4300A *Sensitive Systems Handbook*.[15] The more sensitive data elements (*e.g.*, person handle, DOB, EDIPI) are hidden from authorized users, except system administrators. All other data elements are available to authorized MGMT Cube users, regardless of job function.

Privacy Risk: There is a risk that MGMT Cube will collect more information about individuals than is needed for conducting the analysis and decision-making the system is designed to support.

Mitigation: This risk is partially mitigated. The data elements collected from HSCB EIE and ISMS are reviewed annually by the MGMT Cube Executive Steering Committee and working group to ensure data remains relevant for reporting needs, and if so, then the data elements are reauthorized for another year. If data attributes are deemed no longer necessary for reporting needs, then those data attributes will be purged. Additionally, MGMT Cube minimizes risks by either not accepting sensitive information about people from source systems or restricting access to that information to only MGMT Cube system administrators as detailed at the end of the Overview section of this document.

Privacy Risk: There is a risk that MGMT Cube will combine data elements from HCBS EIE and ISMS, including PII taken from both systems, to create a more comprehensive report that each individual source system is unable to do alone.

Mitigation: This risk is partially mitigated. Although the same PII data elements are collected from both HCBS EIE and ISMS (*e.g.*, person handle and DOB), this is done to ensure that individuals are accurately represented in aggregated analytic reports. In both cases, person handles and dates of birth are hidden from authorized MGMT Cube users, but retrievable by system administrators. Furthermore, no action is taken on specific individuals based on their PII being in MGMT Cube.

[15] DHS 4300A Sensitive Systems Handbook, *available at* https://www.dhs.gov/publication/dhs-4300a-sensitive-systems-handbook.

Privacy Risk: There is a risk that MGMT Cube contains inaccurate data due to the latency of data transfers and not being the authoritative source system.

Mitigation: This risk cannot be fully mitigated because MGMT Cube does not own the data or the source systems. However, MGMT Cube's data migration automation allows for the CXO source systems to initiate data refresh at the convenience of the CXO.

Additionally, while MGMT Cube may contain inaccurate information about individuals, this information is never the basis to make a personnel decision about an individual.

Section 3.0 Uses of the Information

The following questions require a clear description of the project's use of information.

3.1 Describe how and why the project uses the information.

The data in MGMT Cube are used by analysts and executives to analyze issues and make decisions across Management's CXOs. MGMT Cube does not collect information directly from individuals, but rather aggregates data from Management source systems to create reports on DHS personnel (employees and contractors), such as demographic data, calculations of retirement eligibility, and other macro-level data analyses. Many of these reports are in response to requests by Management's stakeholders seeking information related to their job duties. Examples of typical data requests from Management customers include:

- Number of DHS federal employees of a certain occupation in a specific location;
- Percentage of DHS federal employees eligible to retire per occupation;
- DHS programs as identified by DHS federal employees potentially impacted in a hurricane zone;
- Numbers of DHS facilities in each city and state;
- Available budget dollars to fund departmental missions;
- Dollars expended by Components from a specific treasury account;
- Investments in the Under Secretary for Management's Master Acquisition Oversight List (MAOL); or
- Dollars obligated to information technology contracts.

3.2 Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how DHS plans to use such results.

No. MGMT Cube does not conduct electronic searches, queries, or analyses in an electronic database to discover or locate predictive patterns or anomalies.

3.3 Are there other components with assigned roles and responsibilities within the system?

Employees from all DHS components may apply for read-only access to MGMT Cube. However, access is only granted upon compatible mission requirements that require access to such data. Approval for access is required by the requester's immediate supervisor, CXO representative, and the MGMT Cube team. Only certain individuals in Management and its reporting components have MGMT Cube system administrator rights.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk associated with individuals gaining unauthorized access to information in MGMT Cube.

Mitigation: This risk is partially mitigated. All BIaaS IT security and policy controls comply with the DHS 4300A *Sensitive System Handbook*.[16] Specific security controls require database accounts to access MGMT Cube on a need-to-know basis, subject to the approval of the system owner, system administrators, and the ISSO. By signing the *MGMT Cube Rules of Behavior*, all authorized users acknowledge that they have read and understand the rules for accessing MGMT Cube and its data, including the consequences for failing to comply with the rules, which range from a verbal or written warning, removal of system access, and reassignment to other duties, to criminal prosecution, civil liability, or termination. MGMT Cube also contains an audit history log that details the data accessed, which users accessed it, and when MGMT Cube was queried.

Section 4.0 Notice

The following questions seek information about the project's notice to the individual about the information collected, the right to consent to uses of said information, and the right to decline to provide information.

4.1 How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

MGMT Cube does not collect information directly from individuals, but aggregates data from Management source systems to create analytic reports on DHS personnel (*e.g.*, demographic data, calculations of retirement eligibility, and other macro-level data analyses). As such, other than the notice provided by the privacy-sensitive source systems (*i.e.*, HCBS EIE and ISMS), there is no specific notice provided to personnel whose information is aggregated in reports and dashboards generated by MGMT Cube.

[16] *Available at* https://www.dhs.gov/publication/dhs-4300a-sensitive-systems-handbook.

Notice is provided by the publication of this Privacy Impact Assessment, and the System of Records Notices that cover MGMT Cube's source systems identified above in Section 1.2.

4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

The HCBS EIE and ISMS source systems provide individuals with notice and an opportunity to provide consent to the stated uses of their information (*e.g.*, background checks conducted prior to beginning work as an employee or contractor). Although individuals do not have a separate opportunity to consent to the use of their data in MGMT Cube, they may seek correction of their data in the appropriate source system(s). However, information used by MGMT Cube is aggregated to generate overall counts of DHS employees by broad categories, such as age range, ethnicity, and years of service and is therefore difficult to associate to any one individual.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that individuals providing information to OCHCO and OSCO do not have notice that some of their personal information will be visible in MGMT Cube.

Mitigation: This risk is partially mitigated by publication of this PIA, and through the SORNs referenced in Section 1.2. Although there is no specific notice of the use of information in MGMT Cube at the point of collection, DHS employees and contractors may reasonably expect that limited personal information may be used for administrative and managerial functions.

Section 5.0 Data Retention by the Project

The following questions are intended to outline how long the project retains the information after the initial collection.

5.1 Explain how long and for what reason the information is retained.

Reports created by MGMT Cube are covered by the NARA GRS 5.2, item 020, *Intermediary Records*.[17] Additionally, MGMT Cube is working to align its data retention policy with the NARA-approved data retention policies of the source systems from which MGMT Cube receives data.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk that the information in MGMT Cube will be retained longer than necessary or inconsistently with the records schedule applicable to that data.

Mitigation: This risk is not fully mitigated. As discussed, the reports generated from MGMT Cube have a historical use beyond their initial creation (*e.g.*, how many DHS employees

[17] *See* https://www.archives.gov/files/records-mgmt/grs/grs05-2.pdf.

live within 20 miles of Washington, D.C.), therefore the business use for the data is likely to continue for many years beyond its creation. MGMT Cube personnel are currently working with the source system data owners to align with their retention requirements.

As discussed in Section 2.5, MGMT Cube personnel conduct an annual review for each data attribute to ensure the data is still relevant for reporting needs. If data attributes are deemed no longer necessary for reporting needs, then those data attributes will be purged.

Section 6.0 Information Sharing

The following questions are intended to describe the scope of the project information sharing external to the Department. External sharing encompasses sharing with other federal, state and local government, and private sector entities.

6.1 Is information shared outside of DHS as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

MGMT Cube information may be shared to assist in its response to inquiries from Congress and external agencies. In such circumstances, MGMT Cube reports may be included in the Department's response to external inquiries.

6.2 Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

Non-aggregated data is not generally shared outside of the department by MGMT Cube. However, the MGMT Cube source system SORNs permit the sharing of the information MGMT Cube receives with external entities. The routine uses in the SORNs define the circumstances for when information may be shared externally. A complete list of the routine uses can be found in the listed SORNs. The following are two examples of the information sharing permitted by routine uses:

- Information may be shared with an agency, organization, or individual for the purpose of performing audit or oversight operations as authorized by law, but only such information as is necessary and relevant to such audit or oversight function. (*Routine Use D,* DHS/ALL-023 Personnel Security Management System of Records).
- Information may be shared with contractors and their agents, grantees, experts, consultants, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for DHS, when necessary to accomplish an agency function related to this system of records. (*Routine Use JJ,* OPM/GOVT-1 General Personnel Records).

6.2 Does the project place limitations on re-dissemination?

Yes. The source system data owners must provide prior approval for any re-dissemination of their data in MGMT Cube.

6.3 Describe how the project maintains a record of any disclosures outside of the Department.

Disclosures and reports made outside of DHS are captured in MGMT Cube's SharePoint Request Library. The MGMT Cube's SharePoint Request Library contains a log of past reports for report reuse, statistical analysis, and accomplishments.

6.4 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that individuals authorized to access MGMT Cube will conduct unauthorized activities, such as extracting and sharing information with unauthorized recipients.

Mitigation: This risk is partially mitigated. All authorized users are required to sign a *MGMT Cube Rules of Behavior* document prohibiting such practices. Punishments for failing to comply with these Rules of Behavior range from a verbal or written warning, removal of system access, and reassignment to other duties, up to criminal prosecution, civil liability, or termination. Authorized users receive training specific to MGMT Cube, which covers the practices addressed herein. MGMT Cube also contains an audit history log that details the data accessed, which users accessed it, and when MGMT Cube was queried.

Section 7.0 Redress

The following questions seek information about processes in place for individuals to seek redress which may include access to records about themselves, ensuring the accuracy of the information collected about them, and/or filing complaints.

7.1 What are the procedures that allow individuals to access their information?

Individuals may seek access to their records by consulting the redress procedures in the appropriate SORNs for the applicable source systems. DHS employees and contractors may contact system administrators at mgmtcube@hq.dhs.gov to determine which CXO system owner to contact.

An individual may also seek access to his or her records by filing a Privacy Act or Freedom of Information Act (FOIA) request. Only U.S. citizens, lawful permanent residents, and covered persons from a covered country under the Judicial Redress Act (JRA) may file a Privacy Act request. Individuals not covered by the Privacy Act or JRA still may obtain access to records

consistent with FOIA unless disclosure is prohibited by law or if the agency reasonably foresees that disclosure would harm an interest protected by an exemption. If an individual would like to file a Privacy Act or FOIA request to view his or her record, he or she may mail the request to the following address:

Chief Privacy Officer/Chief Freedom of Information Act Officer
Department of Homeland Security
245 Murray Drive, S.W.
STOP-0655
Washington, D.C. 20528

These requests must be in writing and include the requestor's daytime phone number, email address, and as much information as possible of the subject matter to expedite the search process. Specific FOIA contact information can be found at http://www.dhs.gov/foia under "Contact Information." 6 C.F.R. Part 5, Subpart B, provides the rules for requesting access to Privacy Act records maintained by DHS.

7.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

The procedures by which data subjects may request amendment of their information are explained in the source system SORNs. If information is corrected or removed in the underlying source systems, the updated data will be reflected in MGMT Cube when the data is extracted.

7.3 How does the project notify individuals about the procedures for correcting their information?

DHS provides a general notice to the public on how to file a Privacy Act request available at: http://www.dhs.gov/file-privacy-act-request. DHS employees and contractors may also contact MGMT Cube administrators at mgmtcube@hq.dhs.gov.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that individuals will not be able to correct inaccurate information about them in MGMT Cube.

Mitigation: This risk is partially mitigated. All information in MGMT Cube is taken from the individual CXO source systems, which is where redress should be sought. For information about which source system provided specific data elements, individuals may contact MGMT Cube administrators at mgmtcube@hq.dhs.gov.

Additionally, while MGMT Cube may contain inaccurate information about individuals, this information is never the basis to make a personnel decision about an individual.

Section 8.0 Auditing and Accountability

The following questions are intended to describe technical and policy based safeguards and security measures.

How does the project ensure that the information is used in accordance with stated practices in this PIA?

Each source system owner and the MGMT Cube system owner signs a Memorandum of Understanding (MOU), which designates a representative within its organization to facilitate MGMT Cube authorizations and initiatives. One of the functions each representative performs is to review all reports and dashboards to ensure information is appropriately aggregated, so individuals cannot be identified. All authorized users must also review and sign the *MGMT Cube Rules of Behavior* and receive training specific to MGMT Cube.

8.2 Describe what privacy training is provided to users either generally or specifically relevant to the project.

MGMT Cube system administrators are instructed on quality constraints and limitations regarding sensitive data that are based on various administrative protocols. DHS also provides annual mandatory privacy and security awareness training to all employees and contractors on the proper collection, use, and safeguarding of PII.

8.3 What procedures are in place to determine which users may access the information and how does the project determine who has access?

Access to MGMT Cube is granted through a formal multi-step approval process requiring approvals from the requester's immediate supervisor, source system representative, and the MGMT Cube technical team. This approval process is documented in the MGMT Cube Standard Operating Procedures and summarized below:

1. A prospective new user must complete and submit to the MGMT Cube team a packet consisting of a complete Access Request Form, written approval from the user's immediate supervisor, and a copy of the *MGMT Cube Rules of Behavior* signed by the prospective user.
2. The MGMT Cube team reviews the prospective user access request to ensure: the Access Request Form is completed in its entirety; the *MGMT Cube Rules of Behavior* is signed; the individual's immediate supervisor has provided approval; and sufficient MGMT Cube licenses exist.
3. The source system representative reviews the user access request to ensure the prospective user has a valid need to access MGMT Cube and the data therein.

4. If the source system representative approves the access request, the request is forwarded to the system administrator, who validates that all necessary information is included in the request before creating a user account with the necessary permissions.
5. Access is granted once the user completes the mandatory training requirements.

8.4 How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within DHS and outside?

MGMT Cube has an executive steering committee that reviews and approves all strategic planning documents, including information sharing agreements, MOUs, and other privacy compliance documentation. These documents are also reviewed by the program manager, project sponsors, and other program stakeholders, to include the DHS Privacy Office when necessary. New access, additional data loads, and other project priorities are managed by a MGMT Cube working group. Review and approval processes related to MGMT Cube are defined in the MGMT Cube Standard Operating Procedures.

Responsible Officials

Robert C. King
Program Manager, Management Cube
Office of the Chief Readiness Support Officer
Department of Homeland Security

Alicia Lewis
Deputy Program Manager, Management Cube
Office of the Chief Human Capital Officer
Department of Homeland Security

Approval Signature

Original, signed copy on file with the DHS Privacy Office.

_____

Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security