Privacy Impact Assessment Update
for the

Procurement Request Information System Management (PRISM)

DHS/ALL/PIA-013(b)

April 24, 2017

Contact Point
Greg Naylor
Oversight and Strategic Support/Acquisition Systems Branch
Office of the Chief Procurement Officer
(202) 447-5325

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

Abstract

The Department of Homeland Security (DHS) Management Directorate, Office of the Chief Procurement Officer (OCPO) is the owner of the Procurement Request Information System Management (PRISM) contract writing management system. PRISM is a software product that provides full procurement lifecycle support including all phases from advanced acquisition planning through contract closeout. PRISM provides procurement and acquisition support at the desktop through a secure browser only, giving global access to all DHS procurement personnel and their customers. The purpose of this Privacy Impact Assessment (PIA) Update is to reflect changes due to the addition of the Federal Emergency Management Agency (FEMA) as a user of the PRISM system, and FEMA's use of a special feed of PRISM data. A detailed discussion of the PRISM system and the personally identifiable information (PII) it collects may be found in the previously published PIAs.[1]

Introduction

The PRISM system has operated at DHS since 2004, and provides comprehensive, Federal Acquisition Regulation (FAR)-based acquisition support for DHS entities. PRISM is a contract writing management system used by the Office of Procurement Operations (OPO), U.S. Immigration and Customs Enforcement (ICE), U.S. Citizenship and Immigration Services (USCIS), Federal Law Enforcement Training Center (FLETC), Office of the Inspector General (OIG), and now FEMA. Each DHS component listed uses the same version of PRISM and performs the same procurement-related functions. The same set of user roles is employed by all users of PRISM.

The DHS OCPO/Acquisition Systems Branch makes PRISM available to use for procurement-related functions on a shared basis. Although all DHS component users of PRISM share the same instance of the system, the procurement functions of each DHS component are isolated from one another so that each component cannot access the work product of another component. The component users of PRISM pay for their service based on their usage. Component users of PRISM can spread the cost of system operation among multiple users thus increasing efficiency. The functional capabilities of PRISM are available equally to all component users.

A separate instance of the PRISM system was also implemented for the Office of Selective Acquisition (OSA) on the C-LAN in 2012.[2] C-LAN operates as the DHS IT classified network for Top Secret/Sensitive Compartmented Information (TS/SCI) level procurement operations. C-LAN

[1] For the previously published PRISM PIAs, please *see* https://www.dhs.gov/publication/prism.
[2] For information about this separate instance of PRISM, please *see* DHS/OCPO/PIA-013(a) PRISM System (November 10, 2011), available at https://www.dhs.gov/publication/prism.

ensures that Homeland Security intelligence missions are conducted appropriately, without compromising confidentiality, availability, or integrity of sensitive national security intelligence information.

Reason for the PIA Update

This PIA is being updated because FEMA has been added as a new user of the original PRISM system. FEMA will use the PRISM application as all other DHS component users.[3] However, FEMA also requires a special feed of PRISM data into another FEMA system. This PIA Update reports in detail about that unique user feed.

FEMA chose PRISM because it is a Commercial-off-the-Shelf (COTS) software product that provides full procurement lifecycle support including all phases from advanced acquisition planning through contract closeout. FEMA's use of PRISM will eliminate existing manual processes and support the agency's acquisition and assistance management lifecycle.

FEMA had previously used two separate financial systems: Automated Acquisition Management System (AAMS) and Web-based Integrated Financial Management Information System (WebIFMIS).[4] FEMA is replacing the functionality of AAMS with the use of the PRISM system. AAMS has been decommissioned by FEMA, and all of the active contract information in AAMS was migrated to PRISM in a one-time transfer.

PRISM also provides the capability to interface with financial systems that are critical to the acquisition processes. The scope of the FEMA/PRISM initiative requires data exchange from DHS-owned PRISM to FEMA's WebIFMIS. Although FEMA will still maintain some independent financial system capabilities through WebIFMIS, PRISM will share limited data with WebIFMIS when required. Formerly known as IFMIS, WebIFMIS processes payroll, travel, credit card, and disaster assistance payments, and other accounting-related transactions such as commitments, obligations, expenditures, and advanced charges. WebIFMIS collects information on grantees, vendors, employees (for payroll and travel), and contractors. The system also generates report invoices, payment receipts, and cash receipts. The WebIFMIS platform is web-accessible to only DHS and FEMA internal users.

There is no direct connection between PRISM and WebIFMIS; the data is passed from PRISM through the PRISM Procurement Financial Interface (PFI) to the FEMA Service-Oriented

[3] For more information about how PRISM is used at DHS, please *see* DHS/OCPO/PIA-013 PRISM System (June 4, 2009), *available at* https://www.dhs.gov/publication/prism.
[4] For more information about WebIFMIS, please *see* DHS/FEMA/PIA-020 WebIFMIS (Integrated Financial Management Information System), *available at* https://www.dhs.gov/publication/dhsfemapia-020a-web-ifmis-integrated-financial-management-information-system.

Architecture (SOA) Financial Services (SFS) application and to WebIFMIS. Vendor and contract data is only passed in the direction from PRISM to WebIFMIS. The only information passed from WebIFMIS to PRISM is a "pass" or "fail" response back to PRISM when a transfer of data occurs. This pass-back is in place to ensure that the two systems know when data has been transferred successfully or unsuccessfully.

Privacy Impact Analysis

The System and the Information Collected and Stored within the System

The information that is collected, used, disseminated, and maintained in the system has partially changed as part of this update. An additional user (FEMA) has been added to the PRISM system, and additional vendors with vendor point of contact information have been added to the system, but this type of information is the same as what PRISM already maintains. Most vendor information is pre-loaded into PRISM via electronic download of Central Contractor Registration[5] (CCR) database data on a monthly basis through a secure procedure.

FEMA has also been added as a recipient of information from the PRISM system. AAMS was dispositioned and its contracting data was transferred to PRISM. The information that was part of this one-time migration included the same contracting information that PRISM already maintains. FEMA's WebIFMIS will remain a stand-alone system that will continue to receive data from PRISM when required.

The information that PRISM transfers to WebIFMIS includes the following:

- Vendor information (e.g., vendor code, points of contact, contact information, Data Universal Numbering System (DUNS) number,[6] Taxpayer Identification Number (TIN)[7])

[5] Central Contractor Registration (CCR) is the primary registrant database for the U.S. Federal Government. CCR collects, validates, stores, and disseminates data in support of agency acquisition missions. Both current and potential Federal Government registrants are required to register in CCR in order to be awarded contracts by the Federal Government. CCR validates the registrant information and electronically shares the secure and encrypted data with the federal agencies' finance offices to facilitate paperless payments through electronic funds transfer. Additionally, CCR shares the data with Federal Government procurement and electronic business systems.
[6] The Data Universal Numbering System (DUNS) number is unique, key identifier to retrieve vendor information directly from the CCR. The DUNS is not considered PII.
[7] The Taxpayer Identification Number (TIN) is the number used by the Internal Revenue Service (IRS) to uniquely identify a taxpayer. If the owner of a business or vendor is an individual, the TIN may be the individual's Social Security number (SSN). If the business or vendor owner is a corporation or other organization, the IRS assigns a unique TIN to that entity.

- Basic information about a contract/procurement (e.g., quantity, price, type, description, project ID)
- Important dates associated with a contract/procurement (e.g., award date, start date, end date)
- Financial information about the contract/procurement (e.g., payment discounts, payment terms, payment dates)

Despite the changes to the PRISM system, all of the information is still stored in the same manner. Each component shares access to the PRISM application, yet each component's data is logically separated and cannot be freely accessed or shared.

Privacy Risk: There was a risk that the one-time AAMS data transfer into PRISM involved incorrect or missing data, or that not all contracts were properly identified.

Mitigation: To mitigate this risk, the PRISM transition team performed three trial runs in a test environment. Also, the transition team held additional data migrations to capture the contracting data not identified in the initial migrations.

Privacy Risk: There is a risk that information could be electronically intercepted by an unauthorized individual now that PRISM interfaces with a new system, WebIFMIS.

Mitigation: This risk is mitigated through several technical measures. A secure communication channel is established between the PFI middleware[8] and the SFS application. The PFI middleware creates an encrypted connection to a dedicated SFS service URL. The SFS application will send an immediate response back to the PFI middleware as an acknowledgement of receipt containing response code for either success or failure. Information exchange will be encrypted using the Federal Information Processing Standard (FIPS) Publication 140-2 and Advanced Encryption Standard-256 as the minimum standard encryption algorithm.

System administrators ensure that security controls protect information while not being processed or transmitted. Security controls include limiting physical access to information systems, separation of duties, managing credentials, and secure storage of backup media.

Both FEMA and OCPO ensure that virus and spyware detection and eradication capabilities are used as appropriate (e.g., workstations, laptops, servers) and that adequate system access controls are in place and maintained on all components connected to the systems.

[8] Middleware is computer software that provides services to software applications beyond those available from the operating system. It can be described as "software glue." Middleware makes it easier for software developers to implement communication and input/output, so they can focus on the specific purpose of their application.

Uses of the System and the Information

PRISM uses this contracting data to accomplish all stages of acquisition from requirements gathering to contract closeout, workload management, and reporting. PRISM uses the information to create requisitions, solicitations, award documents supporting simplified acquisition and large contract procedures, contract modification documents, interagency agreements, blanket purchase agreements, and basic ordering agreements. Additionally, PRISM uses information to manage the acquisition process by establishing user accounts and tracking workload-related processes on procurement transactions. Reports are generated to track and help manage program area workload and provide information in support of DHS procurement goals and objectives.

PRISM will also continue to transmit select PRISM information to the Federal Procurement Data Systems Next Generation (FPDS-NG)[9] system. PRISM also transmits solicitation and supporting data to FedConnect,[10] including Government contact information to allow bi-directional communication between DHS and potential vendors.

With FEMA added as a recipient of information from the PRISM system, the information is now used to inform FEMA of what AAMS previously did. The interface between PRISM and WebIFMIS, via SFS, replaces the functionality lost with the dispositioning of AAMS.

Privacy Risk: There is a risk that the information transferred to WebIFMIS may be used for a purpose outside of the original collection.

Mitigation: This risk is mitigated through several factors. First, FEMA provides specific training to WebIFMIS users as a means of ensuring the accuracy of data entry and the proper interpretation of data. WebIFMIS also employs business rules throughout the system to verify the accuracy of the transactions. Second, FEMA and OCPO have entered into an Interconnection Security Agreement, which specifies Rules of Behavior and required trainings for users.

Retention

There have been no changes to the retention schedules associated with PRISM data. The addition of the initial AAMS data from FEMA falls under the same retention schedules as the data already maintained by PRISM. Furthermore, WebIFMIS has the same retention schedule as

[9] FPDS-NG is a publicly available database that contains procurement transaction information. PRISM electronically transmits information that does not contain PII or proprietary information to FPDS-NG. This transfer of information is described in DHS/ALL/PIA-013 PRISM, *available at* https://www.dhs.gov/publication/prism.
[10] FedConnect is a full-service web portal, hosted by the vendor Compusearch, which allows DHS to post acquisition opportunities to a central location where vendors can search the opportunities, submit responses, and receive awards. DHS transmits solicitation and supporting data to FedConnect for bid and proposal receipt purposes. PII that is transmitted to FedConnect is limited to Government contact information to allow communication between potential vendors and DHS. This transfer of information is described in DHS/ALL/PIA-013 PRISM, *available at* https://www.dhs.gov/publication/prism.

PRISM. Retention periods of data for contract information vary according to context and circumstance, but, with respect to completed contract files, disposal customarily occurs six (6) years and three (3) months after final payment.

Internal Sharing and Disclosure

With the addition of FEMA, a new sharing initiative has been undertaken. FEMA and OCPO have entered into an Interconnection Security Agreement that establishes individual and organizational security responsibilities for the protection and handling of the information transferred between PRISM and WebIFMIS.

External Sharing and Disclosure

There are no changes for PRISM with regard to sharing of information external to DHS. PRISM will continue to transmit select PRISM information to FPDS-NG and FedConnect.

Notice

There have been no changes to the notice associated with PRISM data. Vendors provide information and are aware that it will be shared by federal agencies as part of the procurement process.

Individual Access, Redress, and Correction

PRISM access, redress, and correction have not changed with this update. No additional privacy risks have been identified with adding new users or a new source to the system. PRISM follows DHS procurement guidance as it pertains to redress and correction.

Technical Access and Security

With all new users, the control of individual access to PRISM is enhanced through the use of automated Rules of Behavior, which includes a list of policies and procedures that users acknowledge in writing prior to gaining a PRISM account. The Rules of Behavior are displayed electronically to all new users prior to initial login and annually thereafter. Users must agree to abide by the Rules of Behavior prior to logging in. If they do not agree, the system will not permit them to log in.

Users of PRISM receive formal training. A training manual is used to guide the training sessions. Training covers the operation of the system from the users prospective and is interactive. Information System Security Officers (ISSO) provide additional training for personnel when there is a significant change in PRISM's security environment, its security requirements, or when an employee's security role changes. Privacy training is also a required National Institute of Standards and Technology (NIST) Special Publication 800-53 control implemented within PRISM. It is the responsibility of the component users of PRISM to provide IT Security Awareness Training to employees that have access to PRISM.

Additionally, audit logs are reviewed on a weekly basis by the PRISM ISSO. The audit logs include the login report, user profile change report, system security change report, deletion audit log report, unreleased audit log report, and the release without validations audit log report. The PRISM ISSO looks for unusual activities that might indicate misuse of the system, such as an excessive number of "release without validation" transactions in a short period of time. If such activities are discovered, the ISSO follows the security incident response procedures provided by Attachment F, Incident Response, in the DHS 4300A Sensitive Systems Handbook.

Technology

In order to facilitate the transfer of information from PRISM to WebIFMIS, several different capabilities are used. The transfer of data is accomplished through the PRISM PFI and the FEMA SFS application. PFI and SFS are middleware systems used to transfer data between PRISM and WebIFMIS.

PFI is established through the connection between PRISM and the SFS middleware. PFI is an Oracle database which resides on the same server as PRISM and is connected to PRISM via a database link. PFI's primary functions are to pull data from PRISM, apply necessary business rules,[11] and facilitate the transfer of data from PRISM to the SFS middleware.

The SFS middleware is considered a minor application of the FEMA SOA General Support System. Its purpose is to provide a generic financial interface to WebIFMIS to allow data to be accepted into WebIFMIS by a number of differentiating systems via the SFS middleware. The SFS middleware is comprised primarily of two components: the SFS Services and the SFS Gateway. The SFS Services component receives requests which originate from PFI. These requests are then sent to the SFS Gateway. The SFS Gateway component transforms the SFS Service requests to be used by WebIFMIS.

[11] A basic example of a business rule would be a date/time format conversion in which the two systems have the same date, but different date formats.

The PFI middleware provides another layer of security because it prevents the two systems from directly communicating with each other. The PFI middleware solution isolates the data so that PRISM and WebIFMIS do not connect directly. WebIFMIS reaches out to the middleware with requests for data, and then the middleware carries out the request to complete the transaction. The middleware prevents the two systems from directly interacting with the data, significantly reducing data breach liability.

Responsible Official

Greg Naylor
IT Project Manager, PRISM System Owner
Office of the Chief Procurement Officer
Department of Homeland Security

Approval Signature

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

_____

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