GSA Facilities at Risk: Security Vulnerabilities Found in GSA's Management of Contractor HSPD-12 PIV Cards

JE16-002
March 30, 2016

Homeland Security Presidential Directive 12 (HSPD-12), issued in August 2004, recognized a need to eliminate the wide variations in the quality and security of identification used to gain access to federal facilities where there is potential for terrorist attacks.

HSPD-12 established a mandatory, government-wide standard for secure and reliable forms of identification issued by the federal government to its employees and contractor employees in order to enhance security, increase government efficiency, reduce identity fraud, and protect personal privacy. Office of Management and Budget implementing instructions for this directive require all federal executive departments and agencies to conduct minimum background investigations and issue Personal Identity Verification (PIV) cards to all employees and contractor employees who require long-term access to federal facilities and/or information technology (IT) systems (see Figure 1).[1]

Federal Information Processing Standards (FIPS) 201, *Personal Identity Verification of Federal Employees and Contractors* (February 25, 2005), was developed to satisfy the standardization requirements of HSPD-12.[2] According to FIPS 201, the PIV card shall contain, at a minimum, at least one security feature that aids in reducing counterfeiting, is resistant to tampering, and provides visual evidence of tampering attempts.[3] PIV card requirements include that the card must:

- Be issued by officially accredited providers;
- Be granted only after an individual's identity is verified;
- Resist fraud, tampering, counterfeiting, and terrorist exploitation;
- Provide rapid electronic verification of personal identity;
- Grant physical access to federal facilities;
- Grant logical access to federal information systems; and
- Protect individual privacy.

Figure 1. Example of a General Services Administration (GSA) HSPD-12 PIV card.

[1] OMB Memorandum M-05-24, *Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors,* August 5, 2005.

[2] FIPS 201 is the standard identified in HSPD-12 that sets out the technical specifications and requirements for a Federal government-wide identity credential for employees and contractors.

[3] *Id.* at 4.1.2.

The Federal Acquisition Regulation, under subpart 52.204-9, Personal Identity Verification of Contractor Personnel, requires contractors to comply with agency personal identity verification procedures that implement HSPD-12, OMB Memo M-05-24, and FIPS 201. The requirements include that the contractor shall account for all forms of government-provided identification issued to contractor employees in connection with performance under the contract, and that the contractor shall return such identification to the issuing agency at the earliest of any of the following, unless otherwise determined by the government:

- When no longer needed for contract performance;
- Upon completion of the contractor employee's employment; or
- Upon contract completion or termination.[4]

It is the policy of the General Services Administration (GSA) to issue PIV cards to all long-term contractor employees – those engaged for more than six months.[5] GSA requires the use of PIV cards to log into agency workstations and access its IT systems and network. GSA is still in the process of integrating the use of PIV cards for physical access to GSA-managed facilities. GSA Office of Mission Assurance (OMA) and its regional staff provide agency-wide leadership and coordination for GSA's security policy, including managing GSA's HSPD-12 PIV card program.

The objective of our evaluation was to assess GSA's process for issuing, managing, and terminating PIV cards to contractor employees and to determine whether key controls over that process are sufficient and effective.

Our evaluation found significant deficiencies in GSA's process for managing GSA issued PIV cards and for ensuring the completion of contractor employee background investigations. In addition, we found deficiencies in GSA's tracking and maintenance of contractor employee background investigation data stored within GSA's Credential and Identity Management System (GCIMS).

[4] FAR subpart 52.204-9 (d) also requires that "the Contractor shall insert the substance of this clause, including this paragraph (d), in all subcontracts when the subcontractor's employees are required to have routine physical access to a Federally-controlled facility and/or routine access to a Federally-controlled information system. It shall be the responsibility of the prime contractor to return such identification to the issuing agency in accordance with the terms set forth in paragraph (b) of this section, unless otherwise approved in writing by the Contracting Officer."

[5] GSA Order CIO P 2181.1, *Homeland Security Presidential Directive-12 Personal Identity Verification and Credentialing*, October 20, 2008.

We surveyed responsible management officials in each of GSA's 11 regions, and conducted site visits to four regions, including 14 GSA-managed facilities. We found that GSA does not consistently collect PIV cards from its inactive contractor employees, and that some contractor employees use expired PIV cards to access GSA-managed facilities. GSA cannot determine the extent of these problems because it does not track data regarding the collection and destruction of expired PIV cards.

We also found that some GSA regions have not been fully successful in issuing PIV cards to all long-term contractor employees. Three of GSA's 11 regions permit exceptions to GSA's PIV policy and do not issue PIV cards to certain types of contractors, such as those who do not require access to GSA IT systems. In such cases, GSA circumvents the policy that requires issuance of PIV cards to all long-term contractor employees by issuing non-PIV building badges.

The system used to manage information about GSA contractor employees, GCIMS, has significant data reliability deficiencies. Data accuracy is critical to ensure contractor employees have an appropriate active or inactive status, a completed and favorable background investigation, and use an unexpired PIV card for facility access.

These security control weaknesses increase the risk of unauthorized access to the 8,603 facilities managed by GSA.[6] Unauthorized access to a federal facility increases the risk of a security event, such as an active shooter, terrorist attack, or theft of government property, as well as exposure of government sensitive and contractor proprietary information.

The OIG makes nine recommendations to address the issues identified in this report (see page 12). The Associate Administrator of the Office of Mission Assurance agreed with our recommendations and initiated corrective actions. Management's comments can be found in their entirety in the Appendix.

[6] As of May 2015, the GSA Public Building Service managed 354 million rentable square feet in 8,603 buildings in all 50 states, six U.S. territories, and the District of Columbia.

Monitoring the contractor employee PIV card cycle, from issuance to destruction, is the responsibility of the GSA official who requests issuance of the card (Requesting Official).[7] In order to issue a PIV card to a contractor employee, the Requesting Official initiates a request for a background investigation. The minimum background investigation required for federal employees and long-term contractor employees is the National Agency Check with Written Inquiries (NACI). The initial portion of the investigation, called a NAC, includes a search of the Office of Personnel Management's Security/Personnel Investigation Index and Defense Clearance Investigation Index, as well as an FBI Name Check and FBI National Criminal History Check (including a fingerprint check). For the complete NACI, the investigating agency checks law enforcement authorities for criminal history and will confirm an individual's past employment, education, places of residence, and references.

For the period covered by this evaluation, the Federal Protective Service (FPS) was responsible for conducting all background investigations for GSA contractor employees needing PIV cards and for determining whether they were fit to work on GSA contracts. If FPS favorably adjudicated the NAC, GSA issued a PIV card to the contractor employee and allowed them to begin work while the full NACI was being completed.

GCIMS, a GSA internal database operated by the Office of the Chief Information Officer, Identity, Credential, and Access Management Division, is the official system of record and is supposed to be the authoritative source of information for PIV card and background investigation processes for all GSA federal employees and contractor employees.[8] GCIMS contains contractor employee personal information as well as whether a contractor employee has an active or inactive status, has been issued a PIV card, and has had a completed background investigation.

When a contractor employee leaves a contract for any reason, the Requesting Official is responsible for revoking their IT access and retrieving all GSA-issued credentials, from either the contractor employee or their company, and forwarding the credentials to the Regional Credentialing Office for disposal.[9]

---

[7] The Requesting Official is the Contracting Officer's Representative (COR) for the contract, but this role may be fulfilled by a project manager, PBS building manager, or local HSPD-12 point of contact as appropriate. GSA Order CIO P 2181.1, *Homeland Security Presidential Directive-12 Personal Identity Verification and Credentialing*, October 20, 2008, at Ch. 4(1)(b).

[8] After reviewing the draft of this report, GSA management reported that GCIMS is operated by OMA; however, GSA has not yet updated the System of Records Notice (SORN) or GSA policy CIO P 2181.1 to reflect this change.

[9] *Id*. at Ch. 4(1)(b)(6).

The following steps must be performed:

Step 1: Contractors (inactive contractor employees or their company) – Return PIV cards to the GSA Requesting Official within 5 business days of the contractor's last day of work.

Step 2: Requesting Officials – Receive all of the inactive contractor employee's GSA credentials including their current PIV card. Inform GSA Security. Inform GSA HSPD-12 Program Management Office. Mail the PIV card to the Regional Credentialing Office for destruction. Request IT access revocation from IT.

Step 3: Regional Credentialing Officers – Destroy the card. Update the contractor's record in GCIMS to an "inactive" status. Inform HSPD-12 Program Management Office and request deactivation of the PIV card from the issuing office.

The Regional Credentialing Offices are part of OMA. The regional OMA staff provides leadership and coordination for emergency management and security policy including: occupant emergency planning, response and recovery, personal identity verification, physical security, personnel security, and suitability activities.

1 GSA does not consistently collect and destroy inactive GSA contractor PIV cards.

We surveyed GSA regional OMA offices to assess compliance with the requirements for collection and remittance for destruction of PIV cards from inactive contractor employees. Ten of the 11 regions reported that Requesting Officials were not consistently collecting PIV cards and mailing them to the Regional Credentialing Office for destruction. We found that compliance challenges centered on the failure of Requesting Officials to notify Regional Credentialing Offices when contractor employees left or were terminated from employment. We also found a lack of consequences for contractors failing to turn in PIV cards.

According to OMA officials, Requesting Officials reported that they did not collect the cards as required because they were too busy, were unaware of the requirement, did not know which contractor employees were on which contract, or did not know how to collect the cards.

We also found instances during our field work of Requesting Officials not collecting PIV cards from inactive contractor employees as required by GSA policy. For example, we identified two inactive contractor employees who had kept their PIV cards for over seven months after their contract with GSA had ended. Federal Acquisition Regulation subpart 52.204-9 requires contractors to return PIV cards when no longer needed for contract performance. Despite this requirement, these contractors retained their PIV cards after they left the contract. The Requesting Official and program managers failed to enforce this requirement, yet told us that they thought these PIV cards had been collected and destroyed.

Although OMA regional staff record PIV card issuance and maintenance actions in GCIMS, they do not record PIV card collection and destruction. According to GCIMS data, since 2007, GSA has issued over 26,000 PIV cards to its contractor employees. Of these, over 5,800 are recorded as “inactive” in GCIMS. GSA is not able to determine if any of these 5,800 cards were actually collected and destroyed because it does not record this information.

OMA does not have a formal process to detect inactive contractor employees and monitor the return of their PIV cards. However, eight of the 11 OMA Regional Credentialing Offices reported to us that they independently perform ad hoc monitoring to ensure that only active contractor employees have PIV cards.

When a contractor employee’s PIV card is not collected and destroyed at the end of a contract, the security risks of unauthorized access to a federal facility significantly increase, particularly when GSA-managed facilities allow access with only a visual (“flash pass”) inspection of the PIV card, rather than

using the electronic security features of the PIV card to verify the contractor's identity.

2 Contractor employees use expired PIV cards to access GSA-managed facilities.

GSA's policy is to replace PIV cards that have expired or are within six weeks of expiration. Under no circumstances are expired PIV cards to be used.[10] However, during our visit to a Level IV federal facility, we observed seven contractor employees using expired PIV cards to access the building (see Figure 2).[11] These cards had expired between six to nine months before we conducted our site visit. The GSA Requesting Official was reportedly unaware that the contractor employees' cards had expired. Upon finding out they expired, the Requesting Official told us that the contractors would be allowed to retain and use the expired cards until they were able to apply for new ones.

All PIV cards expire after five years. However, we identified 1,040 contractor employees with an "active" status in GCIMS who were issued PIV cards more than five years ago. This indicates that these contractor employees are either using expired PIV cards to access a GSA facility or GSA has incorrectly recorded them as "active" in GCIMS.

A contractor employee's PIV card communicates to guard staff, GSA employees, and tenant agencies that they are actively working on a contract and are permitted access to the facility. For "flash pass" facilities – those that allow entrance to employees who show their passes to guard staff rather than pass them through an electronic point of access – use of expired PIV cards increases the risk of unauthorized access.

Figure 2. Both of these expired PIV cards were used to access a Level IV facility.

[10] *Id*. at Ch. 5(2)(a).

[11] FPS conducts Facility Security Assessments of GSA facilities and rates them on a scale of one (lowest risk) to five (highest risk). Based on the security level determination, FPS recommends specific countermeasures to address the facility's risks.

3 GSA does not comply with PIV card issuance requirements.

It is GSA policy that contractor employees who need routine access to GSA IT systems or GSA-managed space for more than six months must have a PIV card.[12] However, in response to our survey and during OIG onsite inspections, eight of 11 OMA Deputy Regional Directors reported that their region has not been fully successful in issuing PIV cards to all long-term contractor employees. Three of the OMA Deputy Regional Directors reported that their regions permit exceptions to the PIV policy and do not issue PIV cards to certain types of contractors, such as those who do not require access to GSA IT systems. In such cases, GSA circumvents the policy that requires issuance of PIV cards to all long-term contractor employees by issuing non-PIV building badges. Two OMA Deputy Regional Directors stated that this practice was implemented because it was thought to be more cost effective and would reduce the risk of not collecting PIV cards when contractor employees leave the contract. GSA regional offices have no authority to disregard GSA policy and HSPD-12 requirements.

Based on a comparison of a sample of building badge data and GCIMS records, we found over 200 instances where GSA issued building badges instead of PIV cards to contractor employees who did not have corresponding GCIMS records. A lack of a GCIMS record indicates that these 200 contractor employees may be actively working in GSA-managed space without the necessary background investigations. This increases the risk that an unfit contractor employee could actively work on a GSA contract and have access to federal facilities. We describe additional issues we found with GSA local building badges in a related report, *GSA Facilities at Risk: Security Vulnerabilities Found in GSA's Use of Facility Specific Building Badges* (JE16-003). In that report, we make recommendations to address our findings that building badges are unsecure, unregulated, and in frequent use at GSA-managed facilities.

4 GCIMS data is inaccurate and incomplete.

As described above, GCIMS is the official system of record and is supposed to be the authoritative source of information for PIV card and background investigation processes for all GSA federal employees and contractor employees. GCIMS contains contractor employee personal information as well as entries indicating whether a contractor employee has an active or inactive status, has been issued a PIV card, and has had a completed background investigation.

We found significant inaccuracies in GCIMS. For example, GCIMS indicated that GSA had over 92,000 active contractor

[12] *Id*. at Ch. 4(2)(a)(5)(a)(iv).

employees. OMA officials reported that this figure is inaccurate and speculated that there are approximately 50,000 active contractor employees, including those that are short term. This demonstrates a serious data reliability issue.

We also found that GCIMS contained inaccurate and incomplete background investigation data for some GSA contractor employees. Our review of contractor employee background investigation data in GCIMS and data provided by FPS found:

- For 638 contractor employees found to be unfit by FPS, GCIMS records did not reflect the negative adjudication results. Of the 638 contractor employees found to be unfit by FPS, 169 had an active status in GCIMS. Nine of these contractor employees had been issued PIV cards. GSA is unable to determine whether the nine PIV cards were collected and destroyed, as it does not track such information.
- Sixty active contractor employees, whose GCIMS records indicated that GSA had issued them a PIV card, had no background investigation information recorded in GCIMS.
- 2,099 active contractor employees with initial investigations (NAC) more than one year old did not have a final (NACI) determination on file. According to FPS officials, it is not unusual for a full NACI background investigation to take up to 90 days to complete, but they would be concerned if a case is still open after several months.

While OMA officials reported that they periodically validate GCIMS data, they are unable to determine if these examples are the result of poor record keeping practices or if there are in fact active GSA contractor employees with non-existent, incomplete, or unfavorable background investigations.[13]

Requesting Officials provide contractor employee information to regional OMA offices, who manually input that information into GCIMS. According to OMA officials, inaccurate data in GCIMS can be the result of insufficient communication regarding a contractor employee's status between the Requesting Officials and the regional OMA offices. OMA officials stated that the OMA Regional Credentialing Officers and Requesting Officials should communicate to ensure that contractor employee information in GCIMS is accurate and complete.

[13] OIG provided OMA management its analysis of the GCIMS data for review.

We found that PIV card Requesting Officials do not consistently collect PIV cards from inactive contractor employees, and that some contractor employees use expired PIV cards to access GSA-managed facilities. GSA cannot determine the extent of these problems because it does not track the collection and destruction of expired PIV cards in GCIMS.

We also found that some GSA regions have not been fully successful in issuing PIV cards to all long-term contractor employees. Three of GSA's 11 regions permit exceptions to GSA's PIV policy and do not issue PIV cards to certain types of contractors, such as those who do not require access to GSA IT systems. In such cases, GSA circumvents the policy that requires issuance of PIV cards to all long-term contractor employees by issuing non-PIV building badges.

The system used to manage information about GSA contractor employees, GCIMS, has significant data reliability deficiencies. Communication between the Requesting Official and OMA is critical to ensure that GCIMS contains accurate and reliable information concerning whether contractor employees have an active or inactive status, have a completed and favorable background investigation, and use an unexpired PIV card to access the facility.

These issues increase the security risk of unauthorized access to GSA-managed facilities, especially those that allow "flash pass" access. Unauthorized access to a federal facility increases the risk of a security event, such as an active shooter, terrorist attack, and theft of government property, as well as exposure of government sensitive and contractor proprietary information.

1. GSA must enforce its policy for Requesting Officials to: 1) notify OMA when a contractor employee they have requested a PIV card for has finished work on a contract, 2) collect PIV cards from inactive contractor employees, and 3) send the PIV card to the regional OMA point of contact for destruction.

2. GSA must enforce Federal Aquisition Regulation subpart 52.204-9, Personal Identity Verification of Contractor Personnel, which requires contractors to account for and return all forms of Government-provided identification at the earliest of any of the following: 1) when no longer needed for contract performance, 2) upon completion of the contractor employee's employment, or 3) upon contract completion or termination.

3. GSA should develop ongoing monitoring controls to detect when the PIV cards of inactive contractor employees and expired PIV cards have not been collected and destroyed.

4. GSA should develop a control to ensure that if contractor employees do not receive a favorable final background investigation, their PIV cards are revoked, collected, and destroyed.

5. GSA should ensure the 169 unfit contractor employeess with active status in GCIMS do not work for GSA and do not have access to GSA-managed facilities.

6. GSA should conduct a full review of GCIMS data to verify that it is current, accurate, and complete.

7. GSA should develop formal processes to ensure that, going forward, contractor employee information in GCIMS is current, accurate, and reliable.

8. GSA should document the collection and destruction of PIV cards in GCIMS.

9. GSA must comply with HSPD-12 and PIV card issuance requirements without exception.

The objective of this evaluation was to determine whether key controls over GSA's process for issuing, managing, and terminating HSPD-12 PIV cards to contractor employees are sufficient and effective. In order to accomplish our objective, we:

- Conducted onsite visits to 14 GSA-managed facilities in four regions;
- Reviewed and analyzed data from GSA's Credential and Identity Management System (GCIMS) as well as building badge system data from the GSA managed facilities visited;
- Interviewed agency management responsible for issuing and managing PIV cards and building badges, including selected GSA regional building and security managers, FPS guards, Federal Acquisition Service management, Contracting Officer's Representatives, OMA staff, and HSPD-12 Managed Service Office staff;
- Conducted a survey of all GSA regional OMA offices;
- Assessed the adequacy and compliance of GSA Central Office and regional offices' facility specific controls, policies, procedures, and guidance related to the issuance, maintenance, and destruction of PIV cards and building badges; and
- Tested key controls over GSA's HSPD-12 processes and building badge systems by using a risk-based approach to judgmentally test a sample of active and inactive GSA contractor employees and assess the accuracy and completeness of related supporting documentation.

Because our testing samples were judgmentally selected, our findings cannot be generalized to the population of GSA contractor employees or the processes in place at all GSA buildings and regions. Although our findings are not generalizable, they are indicative of the serious security risks identified in this report.

Our evaluation was conducted from June 2014 through May 2015 in accordance with the Council of the Inspectors General on Integrity and Efficiency (CIGIE) *Quality Standards for Inspection and Evaluation.*

GSA

OFFICE OF MISSION ASSURANCE

Patricia D. Sheehan
Director
Office of Inspections and Forensic Auditing
Office of Inspector General
U.S. General Services Administration
1800 F Street NW (JE)
Washington, DC 20405

Dear Ms. Sheehan:

The U.S. General Services Administration (GSA) appreciates the opportunity to respond to the GSA Office of Inspector General's (OIG) draft report entitled, *Draft Report - GSA Facilities at Risk: Security Vulnerabilities Found in GSA's Management of Contractor HSPD-12 PIV Cards.* In its draft report, the OIG issued nine (9) recommendations to GSA. The OIG recommends that the Administrator of GSA take the following actions:

- GSA must enforce its policy for Requesting Officials to 1) notify the Office of Mission Assurance (OMA) when a contractor employee they have requested a Personal Identity Verification (PIV) card for has finished work on a contract, 2) collect PIV cards from inactive contractor employees, and 3) send the PIV card to the regional OMA point of contact for destruction.
- GSA must enforce Federal Acquisition Regulation (FAR) Clause 52.204-9, Personal Identity Verification of Contractor Personnel, which requires contractors to account for and return all forms of government-provided identification at the earliest of any of the following 1) when no longer needed for contract performance, 2) upon completion of the contractor employee's employment, or 3) upon contract completion or termination.
- GSA should develop ongoing monitoring controls to detect when the PIV cards of inactive contractor employees and expired PIV cards have not been collected and destroyed.
- GSA should develop a control to ensure that if contractor employees do not receive a favorable final background investigation, their PIV cards are revoked, collected, and destroyed.

U.S. General Services Administration
1800 F Street NW
Washington, DC 20405
Telephone: (202) 501-0800
Fax: (202) 219-1243
www.gsa.gov

- GSA should ensure the 169 unfit contractors with active status in the GSA Credential and Identity Management System (GCIMS) do not work for GSA and do not have access to GSA-managed facilities.
- GSA should conduct a full review of GCIMS data to verify that it is current, accurate, and complete.
- GSA should develop formal processes to ensure that, going forward, contractor employee information in GCIMS is current, accurate and reliable.
- GSA should document the collection and destruction of PIV cards in GCIMS.
- GSA must comply with Homeland Security Presidential Directive (HSPD-12) and PIV card issuance requirements without exception.

GSA agrees with the findings and recommendations of the OIG. GSA will implement corrective actions for the above referenced recommendations; however, at the time of this response to the draft report, GSA has already taken corrective measures on the following:

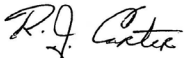
- GSA drafted a *GSA HSPD-12 Contracting Officer (CO), Contracting Officer's Representative (COR), and Program/Project Manager (PM) Policy* reinforcing the roles and responsibilities of the Requesting Officials: CO, COR, and PM. This policy includes the enforcement of HSPD-12 and PIV card issuance for contractors engaged longer than six months that require routine access to GSA facilities and/or information technology (IT) systems (per FAR Clause 52.204-9), the notification of contractor status/data, and the collection of a GSA credential for any contractors that leave GSA.
- GSA drafted a standardized training curriculum and presentation on responsibilities and expectations for COs, CORs and PMs pertaining to HSPD-12 background investigation and credentialing. This training will be published on GSA Online University as an additional training measure.
- GSA implemented training for over 1,000 COs, CORs and PMs pertaining to HSPD-12 background investigation and credentialing. Additional training is currently underway and will continue until all CO, COR and PM staff training is completed.
- GSA initiated the re-write of an existing GSA IT (formerly the GSA Office of the Chief Information Officer) policy (GSA Order CIO P 2181.1, Homeland Security Presidential Directive-12 Personal Identity Verification and Credentialing) that was issued in 2008 and will include accountability of HSPD-12, including but not limited to, the issuance and retrieval of PIV cards.

U.S. General Services Administration
1800 F Street NW
Washington, DC 20405
Telephone: (202) 501-0800
Fax: (202) 219-1243
www.gsa.gov

- GSA began a review of existing IT systems to build a process that will enhance GSA's capabilities to track, collect and destroy PIV cards.
- GSA initiated the process of identifying and resolving the issue of the 169 unfit contractors that are active in GCIMS. GSA obtained the data from the OIG and has been in the process of verifying the information. GSA has found that some of the unfit contractors have already been labeled "inactive" in GCIMS.
- GSA is in the process of updating existing policies and creating new processes to better ensure GCIMS has current, reliable and accurate data.
- GSA will provide timeframes and actions in the final OIG report, once all data is verified.

If you have any questions, please contact me at (202) 604-3412.

Sincerely,



Robert J. Carter
Associate Administrator

U.S. General Services Administration
1800 F Street NW
Washington, DC 20405
Telephone: (202) 501-0800
Fax: (202) 219-1243
www.gsa.gov

OFFICE OF INSPECTOR GENERAL

U.S. General Services Administration

For media inquiries
OIG_PublicAffairs@gsaig.gov
(202) 273-7320

REPORT FRAUD, WASTE, AND ABUSE!

(800) 424-5210

Anonymous Web Form

fraudnet@gsaig.gov

Want to be aware of information the instant it becomes publicly available?

SUBSCRIBE