OFFICE OF INSPECTIONS AND FORENSIC AUDITING

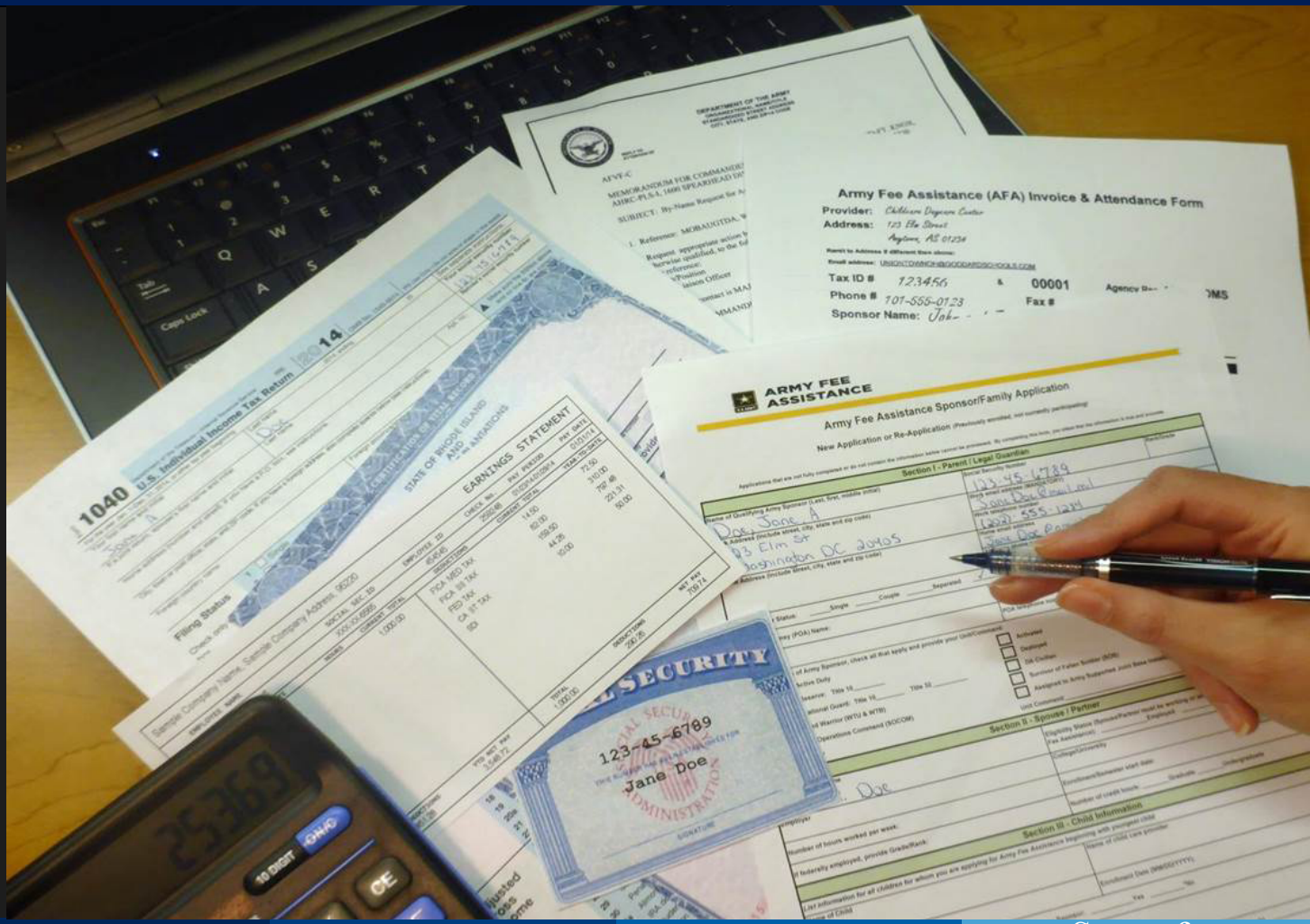
OFFICE OF INSPECTOR GENERAL

U.S. General Services Administration

MANAGEMENT ALERT REPORT

Army Fee Assistance Program: Army Families' Sensitive Information at Risk

Report Number
JE15-003
April 27, 2015



Transmittal Memorandum | Introduction & Background | Findings | Recommendations | Scope & Methodology

U.S. General Services Administration
Office of Inspector General

April 27, 2015

MEMORANDUM FOR: GERARD BADORREK
Chief Financial Officer (B)

FROM: PATRICIA D. SHEEHAN
Director
Office of Inspections and Forensic Auditing (JE)

SUBJECT: Management Alert Report
Army Fee Assistance Program: Army Families' Sensitive Information at Risk
Report Number: JE15-003

The purpose of this report is to alert the CFO to Army families' sensitive information, to include PII, put at risk due to instances of GSA contractor personnel given access to systems and information prior to completing: background investigations or fingerprint checks; privacy training required by GSA policy, and non-disclosure agreements required by the contract. Further, we uncovered inconsistent application of criteria in allowing GSA contractor personnel to telework while working remotely with sensitive information, including PII, of Army families.

We recommend immediate corrective action be taken to minimize further risk to Army families' sensitive information by ensuring that any additional contractor personnel hired to administer this program have appropriate background investigations, training, and non-disclosure agreements completed before being given access to Army families' sensitive information, including PII. Please forward an action plan addressing the recommendations to this office no later than May 27, 2015. Instructions regarding the resolution process can be found in the email that transmitted this report.

If you have any questions regarding this alert report or the ongoing evaluation, please contact me or members of the team at the following:

Patricia Sheehan, Director, patricia.sheehan@gsaig.gov 202-273-4989
Gabrielle Perret, Senior Auditor, gabrielle.perret@gsaig.gov 202- 273-7268

On behalf of the Office of Inspections and Forensic Auditing team, I would like to thank you and your staff for your assistance as we continue this evaluation

Introduction

In February 2015, the General Services Administration (GSA) Office of Inspector General (OIG) began an evaluation of GSA's administration of the Department of the Army (Army) childcare subsidy program. During the course of this ongoing evaluation we identified serious issues that may impact Army families participating in the program.

We found that GSA contractor personnel (contractors) who were hired to process the applications for subsidy payments were able to access sensitive information, including personally identifiable information (PII), without any background investigations or fingerprint checks in place.[1] These contractors were also given access to Army families' PII without first completing all of the privacy training required by GSA policy and without having executed the non-disclosure agreements required by the contract. Further, GSA inconsistently applied criteria in allowing contractors to telework while working remotely with sensitive information, including PII.

GSA program management recently reported that an agreement in principal has been made with the Army to secure funding to hire up to 50 additional contractors. While our evaluation is in progress, we are issuing this management alert report due to the serious nature of these findings and the risks associated with permitting new contractors to work with sensitive information, including PII, without having completed initial background investigations, completed required training, and having executed non-disclosure agreements.

Background

The Army Fee Assistance (AFA or subsidy) program assists eligible Army families in reducing the cost of off-post childcare when on-post options are not available, or when geographically separated from on-post childcare options. AFA is the Army's contribution towards the total cost of off-post childcare, and compensates for some or the entire gap between the on-post rate and the higher off-post rate. AFA allows eligible families to pay fees comparable to those charged at the on-post installation.[2] Categories of eligible Army families include:

- Army Active Duty
- Army Civilians
- Army National Guard – Soldiers on Active Duty Order
- Army National Guard – Dual Status & Non-Dual Status
- Army Reserves – Activated
- Army Reserves – Deployed
- Wounded Warriors
- Survivors of Fallen Soldiers

Since 2003, GSA administered the Army's subsidy program for approximately 200 families who were enrolled in federal childcare centers. GSA also administers the childcare subsidy program for its own employees as well as the programs for the United States Coast Guard, National Park Service, and Customs and Border Protection.[3]

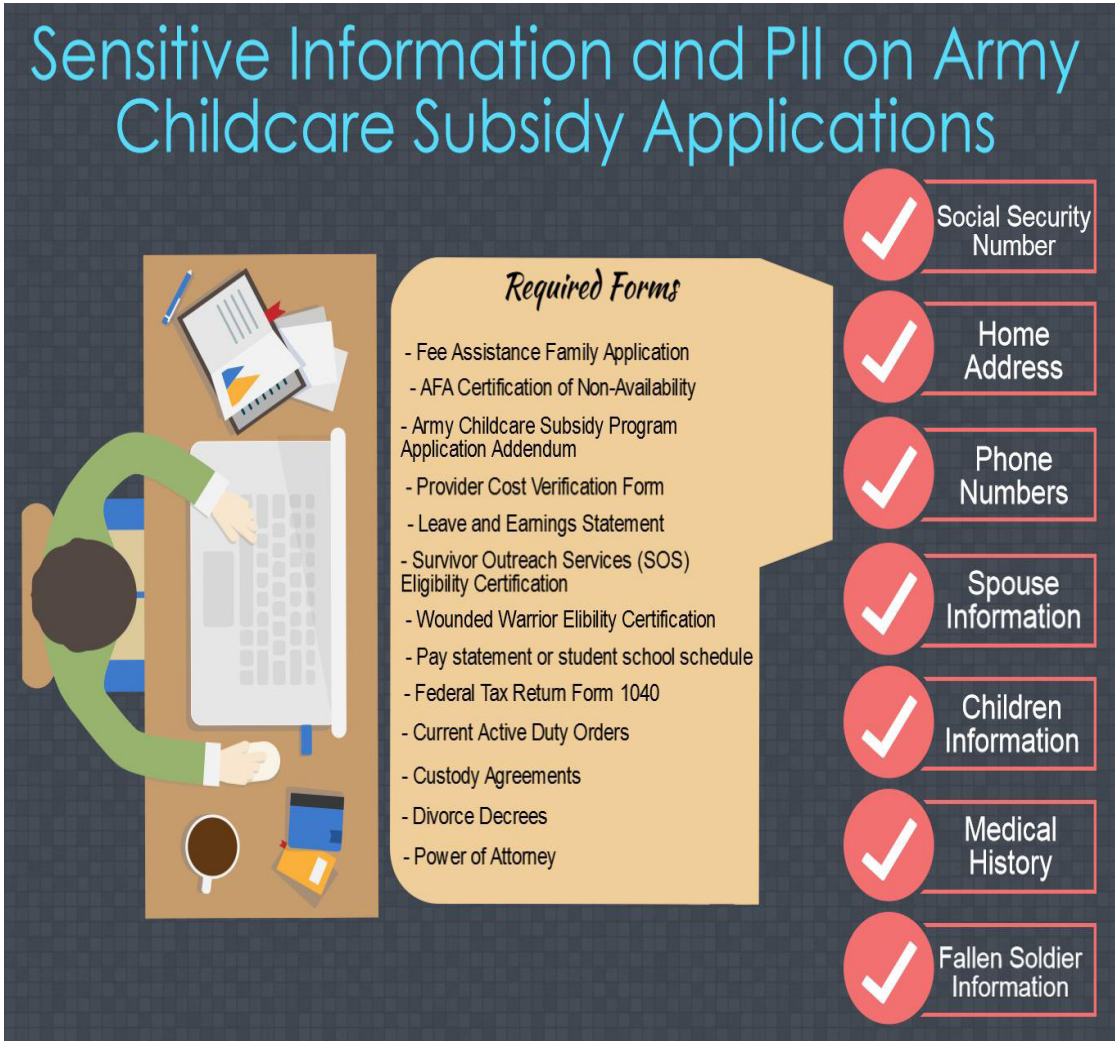


Figure 1. This graphic shows the types of sensitive information and PII elements submitted by Army families to GSA on required childcare subsidy forms.

In early 2014, the Department of the Army expanded its existing interagency agreement with GSA, managed by the Office of the Chief Financial Officer, to include the Army's entire AFA program; a projected increase of an additional 9,000 families who were enrolled in non-federal day care centers. According to GSA officials, Army transferred the additional 9,000 families to GSA's program because GSA provided lower cost services with a higher level of customer service.

Families already enrolled with the prior Army contractor were transferred to GSA on October 1, 2014. Army families new to the subsidy program began to submit applications to GSA on August 1, 2014. To apply for a new subsidy, a family must complete a childcare subsidy application package.[4] Application packages contain sensitive information and PII, see Figure 1.

Upon receipt of a complete application package, GSA determines the amount of the AFA subsidy in accordance with the Army's policies and guidance.

GSA planned to manage this significantly increased workload by hiring contractors in Region 6 and building a custom information technology (IT) system. However, GSA reported significant

setbacks and challenges. When the additional Army families were added, GSA reportedly had five contractors on board when it expected to have approximately 30.[5] GSA officials reported that there were significant delays in processing the initial background investigations of the anticipated contractors, and the IT system was delivered late with limited functionality.

GSA expected enrolled Army families to transition to GSA with no disruption in service or payment of subsidies. However, there have been significant challenges with the program. GSA officials stated that the prior Army contractor sent erroneous and corrupted data that caused significant disruption. However, GSA program officials were unable to provide documentation to support these claims.

By January 2015 GSA had developed a significant backlog of over 11,500 childcare subsidy actionable items waiting processing, see Figure 2. The backlog included:[6]

- over 5,000 family actions unprocessed
- over 3,000 emails unanswered
- over 3,500 phone messages unreturned[7]

The backlog was becoming so unmanageable that a new task order was awarded to a second contractor to provide 20 additional contract employees in Central Office to help clear the backlog.

Figure 2. This graphic shows as of January 2015 a backlog of 11,500 unprocessed family actions, unanswered emails, and unreturned phone messages.

In order to bring the new contractors onboard quickly, the GSA Chief Information Security Officer (CISO) granted special exceptions for the contractors to begin work without having completed the initial background investigation process.

The initial background investigation consists of a National Agency Check, which is a name and fingerprint search of various government and law enforcement databases. This includes a search of the Office of Personnel Management's (OPM) Security/ Personnel Investigation Index, Department of Defense Clearance Investigation Index, FBI Name Check, and FBI National Criminal History Check. Under GSA policy, access to IT systems can be granted after a favorable result of an initial background investigation.[8]

The contractors were given access to GSA networks and systems containing the Army families' sensitive information and PII before initial background investigations were complete.

GSA is planning to migrate the entire GSA childcare subsidy program (to include GSA, Army, Coast Guard, National Park Service, and Customs and Border Protection) to the U.S. Department of Agriculture as part of the financial management line of business (FMLOB) transition. We have not yet determined if GSA has notified the Army families of the planned migration.

In order to migrate the childcare subsidy program to the U.S. Department of Agriculture, GSA must achieve a "steady state."

According to GSA program management, "steady state" means reducing the backlog of actions to 1,800 and processing approximately 60 new actions per day. "Steady state" is expected to be achieved sometime before October 2015.

We plan to report further on these and other issues during our evaluation of the program.

Finding 1. GSA allowed contractors access to Army families' sensitive information and PII without completed initial background investigations, including fingerprint checks.

GSA put the security of Army families' sensitive information, including PII, at risk when it allowed contractors without completed initial background investigations, including fingerprint checks, access to subsidy information.

According to GSA policy, employees and contractors must have a favorable initial background investigation, which includes a fingerprint check, in order to begin work and access GSA IT networks and data.[9] In January 2015, at the request of the Chief Financial Officer, contractors at GSA's Central Office were given special exceptions by the CISO to begin work and access GSA IT networks before the initial background investigation process was completed. These contractors were provided laptop computers pre-configured to permit access to Army families' sensitive information, including PII, on GSA's network, yet the contractors had not completed initial background investigations, including fingerprint checks.

OPM identified issues with three of these contractors. During their initial background investigations, OPM determined further investigative work was required before an adjudication decision could be made.

The OIG conducted an independent criminal background search on the three contractors and identified the following issues:

- Criminal history, including an arrest and a bench warrant
- Financial history, including a recent bankruptcy and financial liens

GSA officials reported that two of the individuals were later removed from the contract, and one left before the results of the OPM initial background investigation was complete.

As part of their normal work duties, the contractors processed Army families' application documents containing sensitive information, including PII. These documents included birth certificates of Army children, tax returns (IRS Form 1040s), leave and earnings statements, school schedules of spouses, locations of childcare providers, and times when children were in childcare. These documents included PII elements and sensitive information such as social security numbers, home addresses, home phone numbers, and bank routing information.

GSA Office of the Chief Information Officer (OCIO) has a waiver process in place for allowing contractors initial IT access before an initial background investigation is completed.[10] Although GSA officials stated that they granted waivers, they were not waivers in accordance with GSA policy. As we read that waiver policy, which incorporates reference to GSA's HSPD-12 standard operating procedure, access should not be given to contractors

before initial background investigations, including fingerprint checks, are completed where their jobs involve handling PII or other sensitive information.[11]

We question the appropriateness of allowing access to contractors whose job duties involve handling PII and other sensitive information before their initial background investigations, including fingerprint checks, are completed.

Finding 2. GSA did not ensure that contractors completed required training and non-disclosure agreements, and did not consistently apply criteria in allowing them to access PII remotely.

According to GSA policy, all employees and contractors must complete "IT Security Awareness and Privacy Training 101" within 30 days of employment.[12] Additionally, all GSA employees and contractors who work with PII, or have access to other people's PII, must also complete "Privacy Training 201."[13]

Before the Central Office contractors were granted access to GSA IT networks, a GSA official in the OCIO advised the childcare subsidy program staff that the contractors would not have access to the GSA online training system to take the required training until two weeks after they started. GSA decided that in-person training would be provided instead. GSA was only able to provide documentation showing that 9 of the 20 Central Office contractors had taken the live "IT Security Awareness and Privacy Training 101." None of the contractors had completed "Privacy Training 201" until program management directed them to do so after the OIG asked whether it had been completed.

Prior to this alert report, similar issues had been raised regarding the GSA childcare subsidy program and protection of sensitive information and PII of Army families. GSA does not have any formal standard procedures in place to validate the identity of callers before discussing sensitive childcare information. Further, the OIG received a hotline complaint alleging that PII was provided during a phone call without the GSA help desk verifying that the caller was authorized to receive the information.

The complainant alleged that they called the GSA childcare subsidy help desk to check on the status of a payment and provided an old ID number assigned by the previous contractor. Without taking any steps to verify the complainant's identity, the complainant alleged that the GSA childcare representative provided the children's names, day care and school locations, and other detailed personal information. Due to the sensitive nature of the Army service member's line of work, the complainant advised the OIG hotline, "I feel they are putting my family in danger." GSA childcare subsidy program management also did not address these concerns in a timely manner as the complainant stated, "I have voiced my concerns and they seem to ignore them over and over."

As a result of the OIG inquiry into this matter, GSA program

management stated that they conducted additional training with staff, but no formal procedures have been established for verifying a caller's identity.

We also found Region 6 contractors working on the Army childcare subsidy program who were permitted to telework, pursuant to the terms of the contract, and access PII remotely for up to three days per week due to space restrictions at a new GSA facility.[14] However, program management had deemed telework inappropriate for the contractors working in GSA's Central Office because of issues working with sensitive information and PII outside of a secure GSA facility.

The two contract teams work on the same tasks and with the same sensitive information and PII. It is unclear why telework poses less risk for the contractors in Region 6 than for the Central Office contractors. Employees and contractors who work with PII while teleworking may increase the risk of a PII breach, especially if staff view sensitive documentation or answer sensitive calls in unsecured locations while teleworking.

According to the Central Office task order, the contractors were also required to sign formal non-disclosure agreements to guarantee the protection and integrity of government information and documents. However, GSA program management had the contractors complete a non-disclosure agreement only after the OIG had asked to review them. Further, GSA is unable to provide non-disclosure agreements for seven of the contractors – to include the three who no longer work on the contract.

1. GSA should enforce its policy CIO P 2181.1, Homeland Security Presidential Directive-12 Personal Identity Verification and Credentialing, October 20, 2008, that states access to moderate-impact applications that contain Privacy Act information should be restricted until full access is granted after the appropriate personnel investigation is completed with favorable results.

2. GSA should enforce its training requirements for contractors handling PII and take immediate action to ensure all childcare subsidy program contractors have completed the required training.

3. GSA should ensure that required non-disclosure agreements are signed by contractors before beginning work.

4. GSA should consistently apply criteria for determining when it is appropriate for personnel to work remotely with PII and other sensitive information.

5. GSA should establish standard procedures to verify the identification of callers before any childcare information is discussed via phone.

To conduct our work for this alert memo, we interviewed GSA program officials, staff, and contractors performing work on GSA's Army childcare subsidy program. We reviewed criteria relevant to the program, including GSA policies and procedures, Army Childcare Subsidy rules and guidelines, the Federal Acquisition Regulation, and contract documents. We also reviewed other types of documentation pertinent to this program, such as OPM background investigation data, law enforcement data, and Army families' subsidy data.

[1] According to GSA Policy and Procedure CIO P 2180.1, GSA Rules of Behavior for Handling Personally Identifiable Information (PII), October 29, 2014, PII is "information about a person that contains some unique identifier, including but not limited to name or Social Security Number, from which the identity of the person can be determined ... The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified."

[2] Army Fee Assistance Family Handbook, page 4/22.

[3] Total families for all agencies were approximately 1,200.

[4] US Army Fee Assistance new applications website: http://www.gsa.gov/portal/category/107399

[5] GSA eventually increased the number of Region 6 contractors to 64 contractors, as of March 2015.

[6] The family actions backlog includes new applications, adding children, removing children, changes to childcare providers, and customer service inquiries. As of April 2015, GSA management reported that the backlog has been reduced to approximately 3,468 actionable items but unreturned voicemails have increased to over 4,500.

[7] Phone messages also include those left for the U.S. Coast Guard childcare subsidy program. GSA was unable to distinguish those left by U.S. Coast Guard from Army families.

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

[9] Id.

[10] GSA failed to meet the requirements of its own waiver process (OCIO Memorandum, HSPD-12 Waiver Request Process for Contractors, March 10, 2008) when it allowed the 20 contractors IT access without a waiver request from the Contracting Officer or Contracting Officer Technical Representative and without waiting the requisite 15 business days for notification of fingerprint check results.

[11] GSA policy CIO P 2181.1, Homeland Security Presidential Directive-12 Personal Identity Verification and Credentialing, October 20, 2008, Chapter 6 (2)(c): Initial access for an employee or contractor should generally include network access and personal IT applications (e.g., desktop applications, network access, Lotus Notes access, and personal and shared mailboxes), shared, and home directory access. It should also include access to low-impact applications as defined by FIPS 199. Access to moderate-impact applications that contain privacy act information should be restricted until full access is granted after the appropriate personnel investigation is completed with favorable results.

[12] GSA Policy and Procedure CIO P 2180.1, GSA Rules of Behavior for Handling Personally Identifiable Information (PII), October 29, 2014, at (3)(a) and (3)(e).

[13] Id.

[14] A GSA program manager temporarily suspended telework for these contractors, effective March 23, 2015, due to production concerns, not because of PII breach concerns. The contractors were told that regular telework schedules will resume when maximum production levels are achieved.

Report cover photo credit: GSA OIG, Office of Inspections and Forensic Auditing.

OFFICE OF INSPECTOR GENERAL
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?