OFFICE OF INSPECTOR GENERAL

Security Concerns with Federal Emergency Management Agency's eGrants Grant Management System

Homeland
Security

November 19, 2015
OIG-16-11

DHS OIG HIGHLIGHTS

Security Concerns with Federal Emergency Management Agency's eGrants Grant Management System

November 19, 2015

Why We Did This Inspection

As part of our audit of the Federal Emergency Management Agency's (FEMA) Assistance to Firefighters Grant (AFG) program, we identified security concerns with FEMA's eGrants grant management system. We are issuing this letter report ahead of our audit report so FEMA can begin to address the security concerns.

What We Recommend

We made two recommendations to FEMA to address security concerns and eliminate deficiencies in its eGrants system.

For Further Information:
Contact our Office of Public Affairs at (202) 254-4100, or email us at DHS- OIG.OfficePublicAffairs@oig.dhs.gov

What We Found

Since 2001, FEMA provided first responder organizations with more than $9 billion through the AFG and Staffing for Adequate Fire and Emergency Response (SAFER) programs. According to FEMA, it began using the eGrants system in 2003 to manage the funds awarded through these programs. However, the eGrants system does not comply with Department of Homeland Security (DHS) information system security requirements. Specifically, access to the eGrants system is not controlled or limited because FEMA instructs grantees to share usernames and passwords within the grantee's organization and with contractors who manage grants. As a result, someone other than the primary point of contact can take action or make changes in eGrants without the grantee's knowledge.

Additionally, in June 2014, DHS's Office of Cyber Security advised FEMA it should not authorize eGrants to operate because it poses an unacceptable level of risk to the agency. FEMA's Chief Information Officer acknowledged the high level of risk posed by system deficiencies and vulnerabilities. Despite the known system deficiencies and risks, FEMA authorized the continued use of the system.

FEMA Response

FEMA concurred with both recommendations. However, FEMA's corrective actions do not fully address the intent of the recommendations. We consider both recommendations open and unresolved.

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Washington, DC 20528/www.oig.dhs.gov

NOV 19 2015

MEMORANDUM FOR: Brian E. Kamoie
Assistant Administrator
Grant Programs Directorate
Federal Emergency Management Agency

Adrian R. Gardner
Chief Information Officer
Federal Emergency Management Agency

FROM: Mark Bell Mark Bell
Assistant Inspector General of Audits

SUBJECT: *Security Concerns with Federal Emergency Management Agency's eGrants Grant Management System*

For your action is our final letter report, *Security Concerns with Federal Emergency Management Agency's eGrants Grant Management System.* We incorporated the formal comments provided by your office in the final report.

The report contains two recommendations aimed at improving the security of FEMA's eGrants grant management system. Your office concurred with both recommendations. Based on information provided in your response to the draft report, and our analysis of FEMA's response, we determined the corrective actions do not fully address the recommendations. Our analysis begins on page 5.

As prescribed by the Department of Homeland Security Directive 077-01, *Follow-Up and Resolutions for the Office of Inspector General Report Recommendations*, within 90 days of the date of this memorandum, please provide our office with a written response that includes your (1) agreement or disagreement, (2) corrective action plan, and (3) target completion date for each recommendation. Also, please include contact information for responsible parties and any other supporting documentation necessary to inform us about the current status of the recommendation. Until we receive and evaluate your response, we will consider the recommendations open and unresolved. Please send your response or closure request to OIGAuditsFollowup@oig.dhs.gov.

Consistent with our responsibility under the *Inspector General Act*, we will provide copies of our report to congressional committees with oversight and appropriation responsibility over the Department of Homeland Security. We will post the report on our website for public dissemination.

Please call me with any questions, or your staff may contact Patrick O'Malley, Director, Office of Audits, at (856) 596-3822.

Background

In fiscal year 2001, Congress established the Federal Emergency Management Agency's (FEMA) Assistance to Firefighters Grant (AFG) program to meet firefighting and emergency response needs of fire departments, nonaffiliated[1] emergency medical service organizations, and other eligible recipients under the AFG program. AFG provides grants directly to local fire departments and other first responder organizations to obtain equipment, protective gear, emergency vehicles, training, and other resources needed to protect the public and emergency personnel from fire and related hazards. In addition to AFG, FEMA manages the Staffing for Adequate Fire and Emergency Response (SAFER) program, which provides grants for hiring, recruiting, and retaining firefighters. Since 2001, FEMA provided first responder organizations $9.8 billion through the AFG and SAFER programs.

According to FEMA, in 2003 it created eGrants as a temporary grant management database for the AFG program. As of 2015, FEMA still uses this temporary system. The system contains information related to applicant or grantee organizations, all aspects of their grants, and associated management of applications and awards. Grantees use the system to apply for, manage, and close grants. FEMA uses the information in the system to review, administer, manage, and close grants; and to communicate with grantees. Since 2003, FEMA processed at least $9.3 billion in AFG and SAFER grants through the eGrants system.

The *Department of Homeland Security's (DHS) Sensitive Systems Policy Directive 4300A* requires that any information system which processes, stores, or transmits sensitive information must include certain automated security controls. These safeguards must ensure the individual accountability of all users. Components must ensure that user access to the system is controlled and limited based on "positive user identification and authentication" (usernames and passwords) before access is permitted. Individual users must not share usernames or passwords. DHS' policy for *Individual Use and Operation of DHS Information Systems/Computers* also specifies that users

[1] As defined at 15 U.S.C. § 2229(a)(7): "nonaffiliated EMS organization" is a public or private nonprofit emergency medical services organization not affiliated with a hospital and does not serve a geographic area in which the Administrator of FEMA finds that emergency medical services are adequately provided by a fire department.

must comply with requirements for logon "identification and authentication" (usernames and passwords).

The directive further requires that systems that do not comply with the sensitive systems policy should not be "authorized to operate" (unless granted an exception or waiver). Designated authorizing officials, with approval of Chief Information Security Officers, issue Authorizations to Operate (ATO) to systems that pass security and other operational assessments. ATOs generally last for 3-year periods.

Results of Review

FEMA's eGrants system does not comply with DHS information system security requirements. Specifically, access to eGrants is not controlled or limited. FEMA instructs its grantees to share eGrants usernames and passwords within the grantee's organization and with outside entities, such as contractors who manage grants. As a result, someone other than the primary point of contact can take action or make changes in eGrants without the grantee's knowledge.

DHS's Office of Cyber Security told FEMA that it should not authorize operation of eGrants because it poses an unacceptable level of risk to the agency. FEMA's Chief Information Officer acknowledged the high level of risk due to system deficiencies and vulnerabilities. Despite the known system deficiencies and risks, FEMA authorized eGrants to continue to operate.

Shared Usernames and Passwords

FEMA's eGrants system does not comply with DHS's information system security requirements regarding individual user authentication. FEMA instructs its AFG and SAFER grantees to share eGrants usernames and passwords with other fire department personnel or contractors. For example, when a grantee delegates aspects of grant management to someone other than the primary point of contact, the grantee must share the username and password. The grantee's account in eGrants only has this one username and password; any other delegates cannot have their own unique usernames or passwords. There is nothing in the system that would prohibit anyone with that username and password from seeing all of an entity's grants, as well as all details of those grants.

As a result, someone other than the primary point of contact can take action or make changes in eGrants without the grantee's knowledge. For example, according to personnel at one fire department, they were unaware their grant management company had used their username and password. The grant management company was able to successfully file an amendment to extend a grant Period of Performance to expend excess funds. The grant management company did not expend the remaining grant funds but closed the grant. The grantee became aware of this activity when it attempted to close out the grant.

In addition, someone other than the primary point of contact, such as contractors or personnel no longer employed by a fire department, can use the grantee's username and password to access eGrants records including sensitive banking information, such as bank account and routing numbers used for direct deposit of grant reimbursements. According to FEMA's eGrants user guide, a username should be generic to an organization, not associated with any one person, and is permanent. The organization's password can be changed in eGrants; however, neither the username nor the password expires.

Information System Security

DHS's Office of Cyber Security identified and reported significant system weaknesses and vulnerabilities, but FEMA allows eGrants to operate even though it poses an unacceptable level of risk to the agency. In July 2014, DHS's Office of Cyber Security issued an AFG Security Assessment Report, which recommended that FEMA not authorize eGrants to operate because it did not comply with policy and had an unacceptable level of risk to the agency. The security assessment identified vulnerabilities related to levels of functionality (user roles), system availability, and out-of-date security patches. FEMA's Chief Information Security Officer told the eGrants authorizing official about the high level of risk eGrants posed to the agency, but the authorizing official issued the ATO anyway.

ATOs for information systems typically cover 3-year periods. Authorizing officials issue ATOs only for systems that fully comply with *DHS' Sensitive Systems Policy*, which eGrants does not. However, according to FEMA, it has issued single-year ATOs for eGrants since 2008. FEMA cannot operate eGrants without an ATO. FEMA does not currently have an alternative system to manage AFG program grants.

Conclusion

According to FEMA, it began using eGrants in 2003 as a temporary grant management system, but it is still operating in 2015. The system poses significant risk to the agency because eGrants does not comply with DHS' policies governing the use of unique usernames and passwords. This may lead to unauthorized personnel making changes in eGrants without the grantee's knowledge. In addition, DHS identified and reported significant system weaknesses and vulnerabilities, but FEMA has not eliminated them. According to program personnel, technical resources allocated to the program have not been adequate to do so, and no alternative system is currently available to manage AFG programs.

Recommendations

Recommendation 1: We recommend that FEMA's Assistant Administrator, Grants Program Directorate and Chief Information Officer ensure that eGrants is compliant with DHS security requirements by issuing unique usernames and passwords to each person authorized to access eGrants in accordance with *DHS Sensitive Systems Policy Directive 4300A* and the policy for *Individual Use and Operation of DHS Information Systems/Computers*.

Recommendation 2: We recommend that FEMA's Assistant Administrator, Grants Program Directorate and Chief Information Officer ensure that eGrants is compliant with DHS security requirements by eliminating the system weaknesses identified by the Office of Cyber Security before evaluating a 2016 ATO.

Management Comments and OIG Analysis

Recommendation 1: Concur. FEMA plans to implement several steps to strengthen the integrity of the usernames and passwords used to access eGrants by strengthening awareness of appropriate behavior. The steps will include implementing an electronic rules of behavior form, requiring passwords be changed every 90 days, and updating the AFG user guide with specific information about prohibited account activities. FEMA plans to implement these changes by October 31, 2015.

OIG Analysis: FEMA's planned corrective actions do not meet the intent of the recommendation. In its comments, FEMA does not specify how or whether additional usernames and passwords will be created for current eGrants users. The response suggests grantees will simply be informed they cannot share their usernames and passwords. FEMA did not discuss a different workflow for addressing username and password requests nor whether a technical assessment of eGrants will be performed to determine how adding additional usernames and passwords will impact the system's current load and capacity. The response neither discusses whether additional programming in eGrants will be necessary, nor does it discuss FEMA's plan to test additional or changed application functionality. FEMA did not specify any proposed consequences for those grantees in violation of DHS and FEMA policies. The timeframe FEMA proposed for corrective action seems aggressive, given the potential complexity of the solution. We consider the recommendation open and unresolved.

Recommendation 2: Concur. FEMA plans to eliminate eGrants system weaknesses by October 31, 2015. Grant Programs Directorate plans to update the AFG Security Assessment Report as each Plan of Action and Milestone (POA&M) is implemented and approved.

OIG Analysis: FEMA's planned corrective actions do not meet the intent of the recommendation. FEMA did not provide sufficient detail about which items on the POA&M will be corrected, in what order of priority; and what evidence will be provided to show the items have been tested and approved for migration into the eGrants production environment. FEMA did not discuss how it will prevent another backlog of items on the POA&M in the future. The timeframe FEMA proposed for corrective action seems aggressive, given the potential complexity of the solution. We consider the recommendation open and unresolved.

Objective, Scope, and Methodology

The Department of Homeland Security (DHS) Office of Inspector General (OIG) was established by the *Homeland Security Act of 2002* (Public Law 107−296) by amendment to the *Inspector General Act of 1978*.

As part of our still ongoing audit of FEMA's AFG program, we identified security concerns with FEMA's eGrants grant management system. Our objective is to determine the extent to which AFG recipients comply with grant requirements and guidance precluding waste, fraud, and abuse of grant funds. The scope of the ongoing audit includes AFG and SAFER grant awards for fiscal years 2010 through 2012.

We identified a statistical sample of grantees within the scope. We conducted site visits and requested data using standardized questionnaires and document requests. We downloaded records directly from eGrants and collected documentation from grantees that is not stored in eGrants. We used a Data Collection Instrument to reconcile FEMA reimbursements with grantee records and categorized the questioned costs we identified.

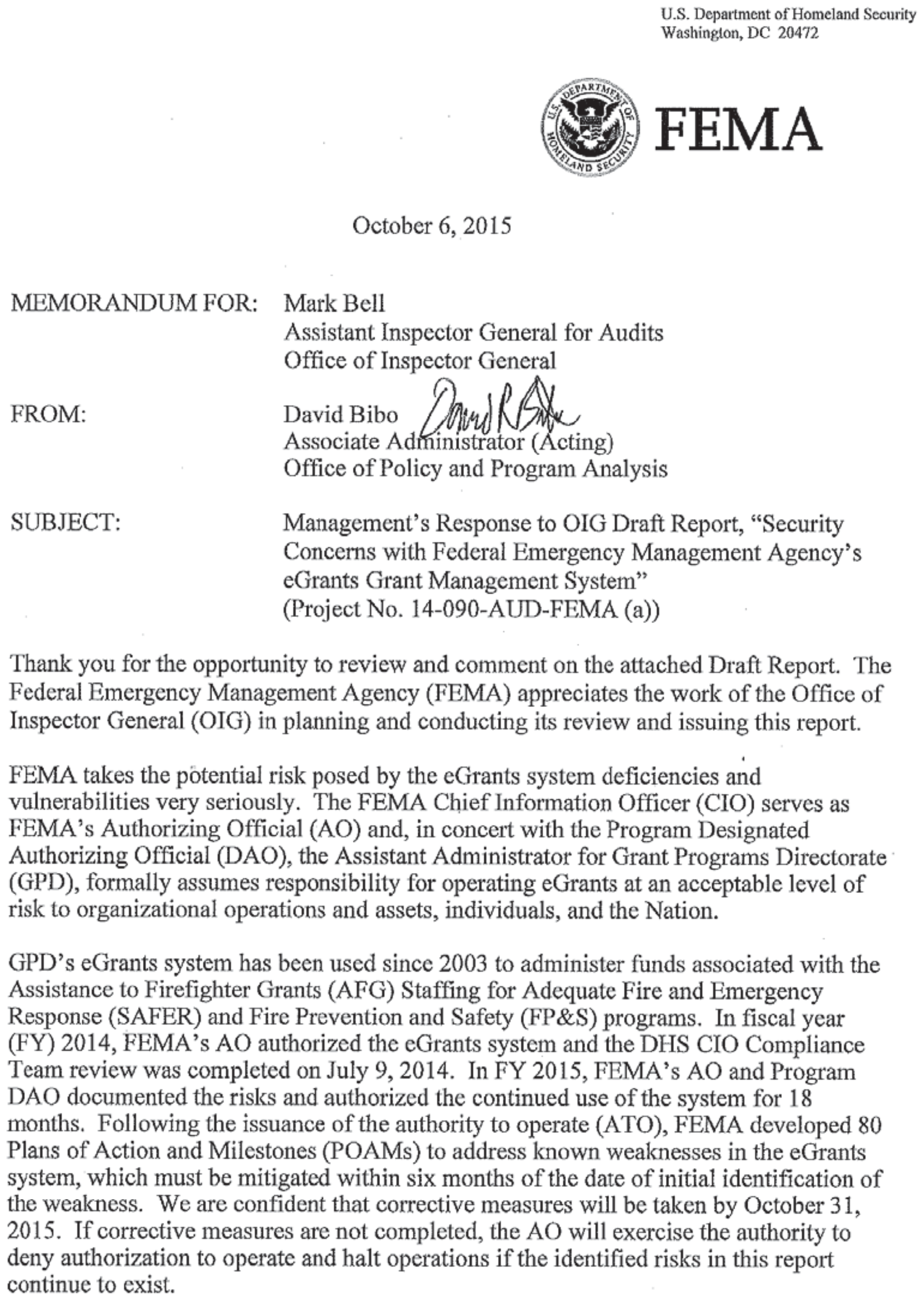
For this letter report, we analyzed the *DHS Sensitive Systems Policy Directive 4300A*; the policy for *Individual Use and Operation of DHS Information*

Systems/Computers; the AFG (eGrants) User Guide; the DHS's Office of Cyber Security AFG Security Assessment Report and Technical Program of Actions and Milestones; and documents detailing the decision to issue a 2014 Authorization (for eGrants) to Operate. We interviewed personnel from FEMA's Grant Programs Directorate; AFG program, technical and operations personnel; the system owner; and grantees.

We conducted this review under the authority of the *Inspector General Act of 1978,* as amended, and according to the Quality Standards for Inspections issued by the Council of the Inspectors General on Integrity and Efficiency.

Office of Audits major contributors to this report are: Patrick O'Malley, Director; Sean Pettersen, Audit Manager; Cecilia Carroll, Audit Manager; Jacque Bear, Program Analyst; Brandon Landry, Program Analyst; Erica Stern, Program Analyst; Philip Emswiler, Program Analyst; Jason Kim, Auditor; Rebecca Mogg, Program Analyst; Kevin Dolloson, Communications Analyst; and Carolyn Floyd, Independent Referencer.

Appendix A
FEMA Comments to the Draft Management Report



U.S. Department of Homeland Security
Washington, DC 20472

FEMA

October 6, 2015

MEMORANDUM FOR: Mark Bell
Assistant Inspector General for Audits
Office of Inspector General

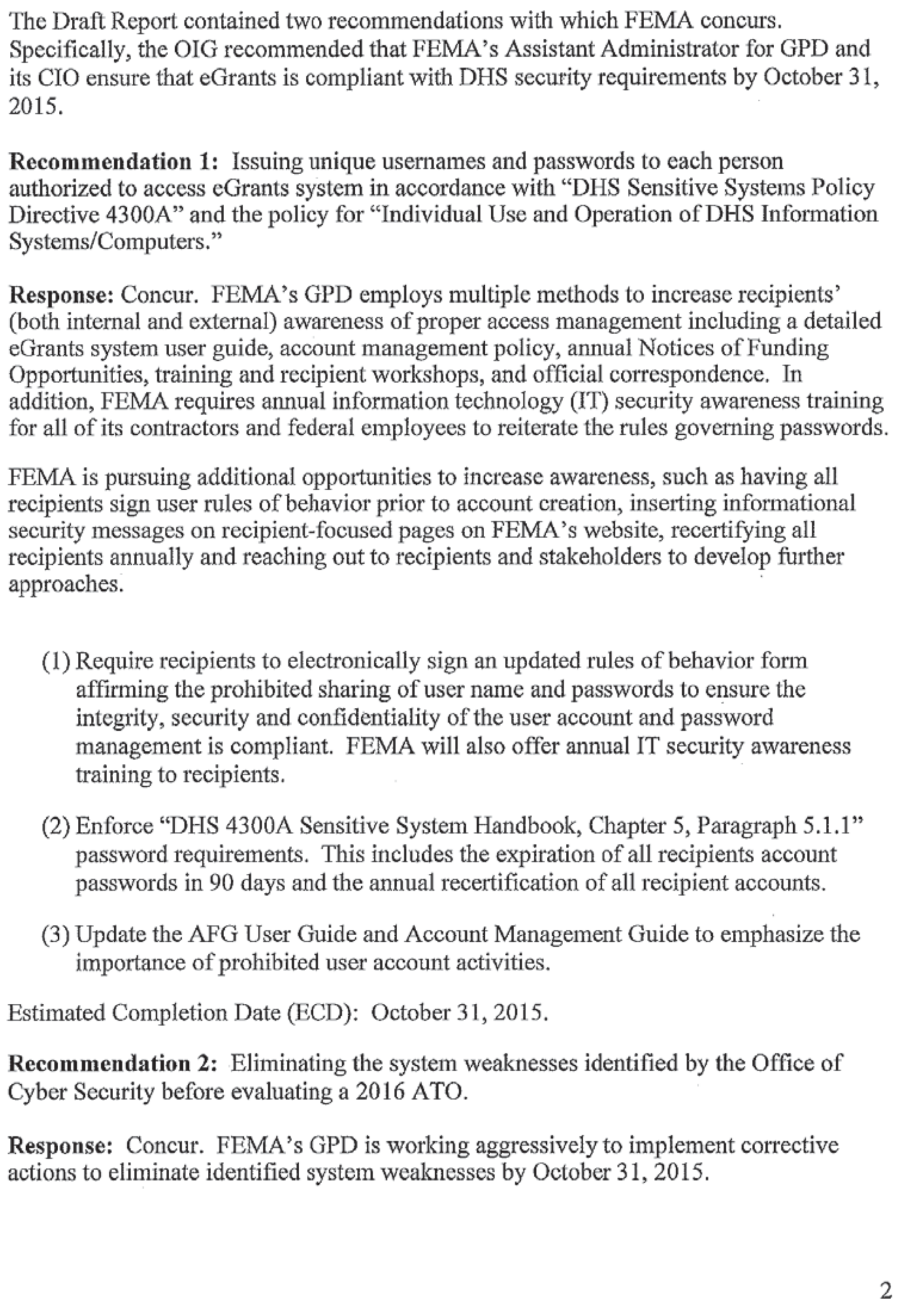
FROM: David Bibo
Associate Administrator (Acting)
Office of Policy and Program Analysis

SUBJECT: Management's Response to OIG Draft Report, "Security Concerns with Federal Emergency Management Agency's eGrants Grant Management System"
(Project No. 14-090-AUD-FEMA (a))

Thank you for the opportunity to review and comment on the attached Draft Report. The Federal Emergency Management Agency (FEMA) appreciates the work of the Office of Inspector General (OIG) in planning and conducting its review and issuing this report.

FEMA takes the potential risk posed by the eGrants system deficiencies and vulnerabilities very seriously. The FEMA Chief Information Officer (CIO) serves as FEMA's Authorizing Official (AO) and, in concert with the Program Designated Authorizing Official (DAO), the Assistant Administrator for Grant Programs Directorate (GPD), formally assumes responsibility for operating eGrants at an acceptable level of risk to organizational operations and assets, individuals, and the Nation.

GPD's eGrants system has been used since 2003 to administer funds associated with the Assistance to Firefighter Grants (AFG) Staffing for Adequate Fire and Emergency Response (SAFER) and Fire Prevention and Safety (FP&S) programs. In fiscal year (FY) 2014, FEMA's AO authorized the eGrants system and the DHS CIO Compliance Team review was completed on July 9, 2014. In FY 2015, FEMA's AO and Program DAO documented the risks and authorized the continued use of the system for 18 months. Following the issuance of the authority to operate (ATO), FEMA developed 80 Plans of Action and Milestones (POAMs) to address known weaknesses in the eGrants system, which must be mitigated within six months of the date of initial identification of the weakness. We are confident that corrective measures will be taken by October 31, 2015. If corrective measures are not completed, the AO will exercise the authority to deny authorization to operate and halt operations if the identified risks in this report continue to exist.



The Draft Report contained two recommendations with which FEMA concurs. Specifically, the OIG recommended that FEMA's Assistant Administrator for GPD and its CIO ensure that eGrants is compliant with DHS security requirements by October 31, 2015.

Recommendation 1: Issuing unique usernames and passwords to each person authorized to access eGrants system in accordance with "DHS Sensitive Systems Policy Directive 4300A" and the policy for "Individual Use and Operation of DHS Information Systems/Computers."

Response: Concur. FEMA's GPD employs multiple methods to increase recipients' (both internal and external) awareness of proper access management including a detailed eGrants system user guide, account management policy, annual Notices of Funding Opportunities, training and recipient workshops, and official correspondence. In addition, FEMA requires annual information technology (IT) security awareness training for all of its contractors and federal employees to reiterate the rules governing passwords.

FEMA is pursuing additional opportunities to increase awareness, such as having all recipients sign user rules of behavior prior to account creation, inserting informational security messages on recipient-focused pages on FEMA's website, recertifying all recipients annually and reaching out to recipients and stakeholders to develop further approaches.

(1) Require recipients to electronically sign an updated rules of behavior form affirming the prohibited sharing of user name and passwords to ensure the integrity, security and confidentiality of the user account and password management is compliant. FEMA will also offer annual IT security awareness training to recipients.

(2) Enforce "DHS 4300A Sensitive System Handbook, Chapter 5, Paragraph 5.1.1" password requirements. This includes the expiration of all recipients account passwords in 90 days and the annual recertification of all recipient accounts.

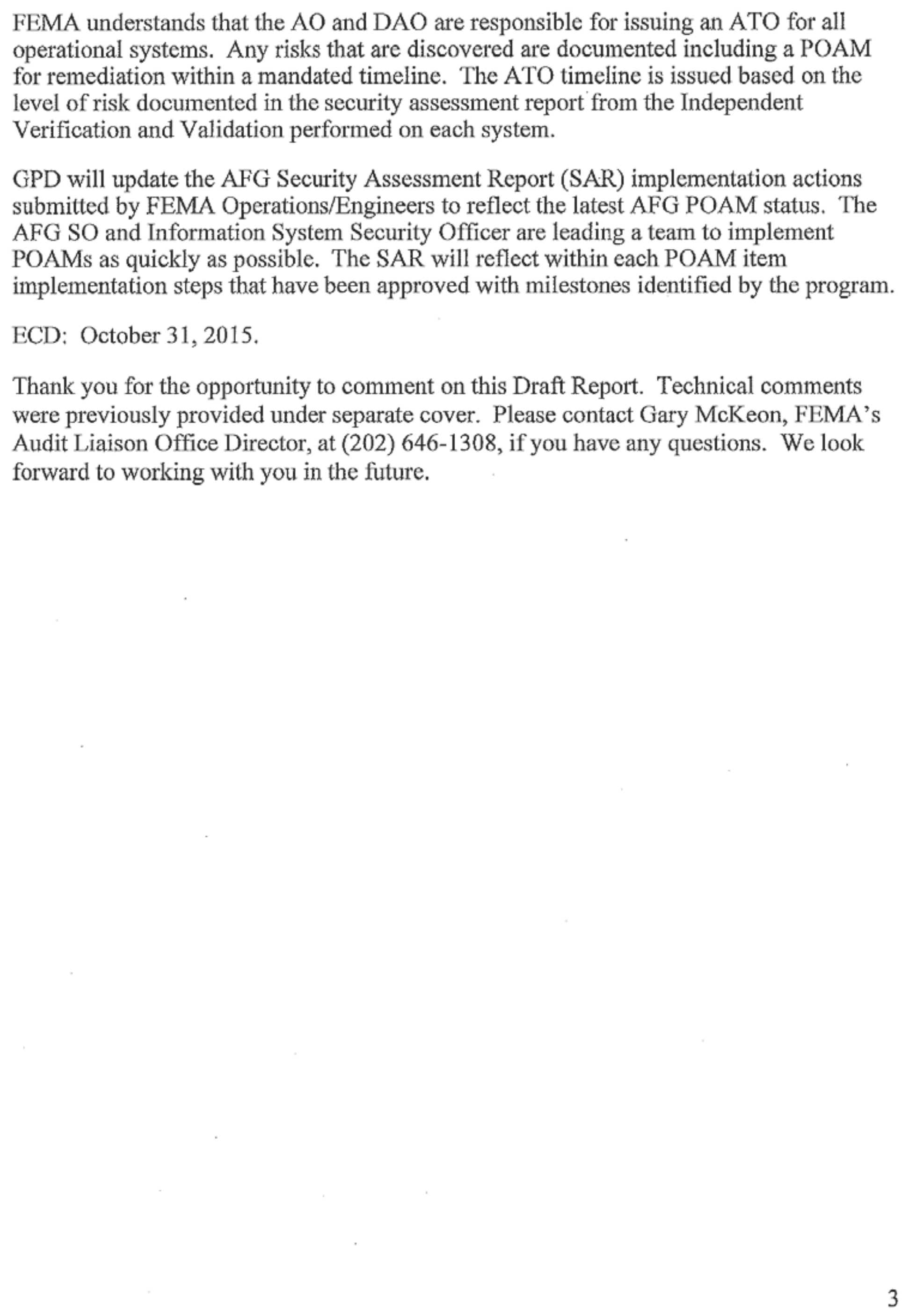
(3) Update the AFG User Guide and Account Management Guide to emphasize the importance of prohibited user account activities.

Estimated Completion Date (ECD): October 31, 2015.

Recommendation 2: Eliminating the system weaknesses identified by the Office of Cyber Security before evaluating a 2016 ATO.

Response: Concur. FEMA's GPD is working aggressively to implement corrective actions to eliminate identified system weaknesses by October 31, 2015.

2



FEMA understands that the AO and DAO are responsible for issuing an ATO for all operational systems. Any risks that are discovered are documented including a POAM for remediation within a mandated timeline. The ATO timeline is issued based on the level of risk documented in the security assessment report from the Independent Verification and Validation performed on each system.

GPD will update the AFG Security Assessment Report (SAR) implementation actions submitted by FEMA Operations/Engineers to reflect the latest AFG POAM status. The AFG SO and Information System Security Officer are leading a team to implement POAMs as quickly as possible. The SAR will reflect within each POAM item implementation steps that have been approved with milestones identified by the program.

ECD: October 31, 2015.

Thank you for the opportunity to comment on this Draft Report. Technical comments were previously provided under separate cover. Please contact Gary McKeon, FEMA's Audit Liaison Office Director, at (202) 646-1308, if you have any questions. We look forward to working with you in the future.

Appendix B
Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
General Counsel
Executive Secretary
Director, GAO/OIG Liaison Office
Assistant Secretary for Office of Policy
Assistant Secretary for Office of Public Affairs
Assistant Secretary for Office of Legislative Affairs
FEMA Audit Liaison

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees

ADDITIONAL INFORMATION AND COPIES

To view this and any of our other reports, please visit our website at: www.oig.dhs.gov.

For further information or questions, please contact Office of Inspector General Public Affairs at: DHS-OIG.OfficePublicAffairs@oig.dhs.gov. Follow us on Twitter at: @dhsoig.

OIG HOTLINE

To report fraud, waste, or abuse, visit our website at www.oig.dhs.gov and click on the red "Hotline" tab. If you cannot access our website, call our hotline at (800) 323-8603, fax our hotline at (202) 254-4297, or write to us at:

Department of Homeland Security
Office of Inspector General, Mail Stop 0305
Attention: Hotline
245 Murray Drive, SW
Washington, DC 20528-0305