UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

Office of the
Inspector General

February 7, 2012

MEMORANDUM FOR JOHN BERRY
Director

FROM: PATRICK E. McFARLAND Patrick E McFarland
Inspector General

SUBJECT: Insecure Password Reset Process on Agency-owned Information Systems (Report No. 4A-RI-00-12-034)

The purpose of this memorandum is to communicate to you the conclusions resulting from our review of a security weakness related to the password change methodology of several information systems operated by the U.S. Office of Personnel Management (OPM). These systems include, but are not limited to, the [redacted]

Executive Summary and Background

[redacted] is a system operated by OPM on behalf of over 50 Federal agencies. [redacted] The nature of these transactions requires [redacted] to store sensitive personally identifiable information (PII) related to its users.

[redacted] are both OPM owned and operated systems that, like [redacted] contain large amounts of PII of federal employees.

In October 2011, OPM's situation room received a tip that [redacted] has a potential security flaw related to the way user accounts are created and the way passwords are reset. Both transactions could be performed by an attacker that knew a [redacted]

In December 2011, the [redacted] system was breached by a malicious attack exploiting the website's password reset feature. The attacker had to enter [redacted] and was able to reset the user's password directly on the [redacted] web interface. The attacker was able to view PII for approximately six different user accounts.

We found that at least one other OPM system, [redacted] has a potentially exploitable password reset function similar to [redacted]. The password reset feature of all three systems could be improved by disabling a user's ability to reset the password directly on the system's public-facing website. A more secure option is for the system [redacted]

[redacted]

We recommend that the Office of the Chief Information Officer review the security of the password reset feature of all OPM systems that contain PII. During this review we also determined that the password complexity requirements for [redacted] are not compliant with OPM policy, and recommend that the appropriate system modifications be implemented.

Scope and Methodology

We reviewed situation room reports related to the [redacted] security breach and the [redacted] vulnerability tip. We also independently tested the process for resetting passwords for [redacted] and [redacted] to evaluate the risk that a user's password could be changed by someone other than the individual owning the account.

Our review was not conducted in accordance with Generally Accepted Government Auditing Standards (GAGAS). The nature and scope of the work performed was consistent with that expected of a GAGAS audit; however, because we consider this to be a review, the documentation, reporting, and quality control standards are not as stringent.

Review Results

Prior to the security breach, a user could reset their [redacted] password by entering [redacted] and [redacted] After the security breach, the password reset feature for [redacted] was modified so that users [redacted] they can no longer conduct the entire transaction directly on the public-facing website.

An OPM employee can create their own [redacted] account at the system's website by entering [redacted]. Passwords for existing accounts can be reset on the website with the same information. During our review, we also determined that [redacted] are not enforced by [redacted] we were able to create a password [redacted]). The OPM Information Security and Privacy Policy Handbook states that information systems must enforce minimum password complexity of at least [redacted], [redacted].

In order to reset an [redacted] password on the system's website, a user must enter the [redacted] [redacted], and [redacted] If a user does not know their [redacted] it can also be obtained directly on the website by entering [redacted] Users must [redacted]. However, like [redacted] these [redacted]

As an additional security feature, [redacted] Although this control would alert an authorized user that their account was breached, it does nothing to prevent an attack from occurring.

We believe that the issues identified in these three OPM systems represent an agency-wide security vulnerability. Although it is typically more convenient for a user to change their password directly on a system's website, this feature increases the risk that an attacker that knows enough information about a user could gain unauthorized access to the system. This risk is increased greatly for systems that have a public-facing website, as anyone with an Internet connection could attempt to hack user accounts. A more secure option is [redacted] Once this additional control is implemented, an attacker would not only need to [redacted].

<u>Recommendation 1</u>

We recommend that [redacted] be modified to enforce the strict password complexity requirements in accordance with OPM's Information Security and Privacy Policy Handbook.

<u>Recommendation 2</u>

We recommend that [redacted] be modified to [redacted] that request to create new accounts or reset the passwords of existing accounts.

<u>Recommendation 3</u>

We recommend that the Office of the Chief Information Officer conduct a review to identify other OPM systems that allow users to [redacted]. The systems identified should be modified so that a [redacted] The [redacted] should also be strengthened so that [redacted]

cc: Elizabeth A. Montoya
Chief of Staff

[redacted]
Director, Executive Secretariat and Ombudsman

Matthew E. Perry
Chief Information Officer

[redacted]
Director
Internal Oversight & Compliance

[redacted]
Deputy Director
Internal Oversight & Compliance

[redacted]
Chief, Policy and Internal Control