AUG 0 3 2015

UNITED STATES DEPARTMENT OF COMMERCE Chief Financial Officer and Assistant Secretary for Administration Washington, D.C. 20230

MEMORANDUM FOR:

Bureau/Operating Unit Chief Privacy Officers and

Principal Human Resources Managers

FROM:

Catrina D. Purvis

Chief Privacy Officer (CPO)

Kevin E. Mahoney

Director for Human Resources Management and

Chief Human Capital Officer

Frederick E. Stephens &

Deputy Assistant Secretary for Administration

SUBJECT:

Procedures on Notifying Management Officials of Individuals

Who Fail to Safeguard Sensitive Personally Identifiable

Information (PII)

This memorandum notifies you to institute coordinated procedures within your respective bureaus to remind managers/supervisors of their responsibilities in addressing situations in which employees and contractors fail to safeguard PII. Your procedures must be consistent with the Department of Commerce PII, BII, and PA Breach Response and Notification Plan, Version 2.0 (July 2013).

On May 22, 2007, the Office of Management and Budget issued a Memorandum for the Heads of Executive Departments and Agencies, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information." The memorandum informed Heads of Departments and Agencies of the urgent need to deal with situations in which individuals demonstrated "egregious disregard or a pattern of error in safeguarding personally identifiable information." A breach of personally identifiable information (PII) incident is considered a violation of a Department of Commerce (Department) security regulation. Managers and supervisors must take appropriate measures to hold Federal employees accountable, and to provide a framework for constructive corrective actions that violate Department security regulations.

For Federal employees, first-line supervisors have the responsibility to determine the appropriate performance or disciplinary action for subordinates who create PII breaches. Disciplinary actions can be guided, in part, by the table of penalties in Department Administrative Order (DAO) 202-751, "Discipline" after consulting with the servicing Employee Relations Specialist and the Office of the General Counsel. For contractors, Contracting Officers (COs) have the responsibility to take appropriate action.

SUBJECT: Procedures on Notifying Management Officials of Individuals Who Fail to

Safeguard Sensitive Personally Identifiable Information (PII)

Page 2

Bureau/Operating Unit Privacy Officers (BPOs) have the responsibility of notifying the employee or contractor, along with his/her supervisory chain of command, or Contracting Officer Representative (COR), as appropriate, when the same individual continues to breach PII.

In order to ensure managers and supervisors are made aware of a PII breach in a timely manner, the following notification procedures are to be used by all BPOs:

For any occurrence of a PII breach, a BPO must notify the employee/contractor involved and an appropriate supervisor or COR in a manner in which they deem appropriate.

In order to ensure all information is provided to a supervisor, the BPO should use the attached templates as a guide to notifying the first- and/or second-line supervisor of a Federal employee, or the COR of a contractor. The BPO shall determine if the PII breach warrants further notifications, and the employee's or contractor's supervisor will determine appropriate action.

Notifications of PII breaches by Federal employees will be escalated by the BPO whenever necessary to ensure that senior management is aware of the situation and the first-line supervisor has implemented appropriate corrective/remedial actions. Such notification may also include a recommendation for prompt removal of the employee's authority to access information and systems that is or contains sensitive PII. Notifications regarding PII breaches by contractors are to be escalated to the CO or higher, to ensure appropriate action is taken.

Please ensure appropriate attention to, and priority of, compliance with these procedures in your Bureau/Operating Unit. Questions about this memorandum should be directed to the Commerce Privacy Program Coordinator, Ms. Lisa Martin. She can be reached at (202) 482-2459 and LMartin1@doc.gov.

Attachments

- Example Notification E-mail 1
- Example Notification E-mail 2 (subsequent occurrences)

cc: Brian D. DiGiacomo Chief, Employment and Labor Law Division

E-mail Notification to Immediate Supervisor/Contracting Officer Representative

FOR YOUR ACTION AND ATTENTION

[Insert Name of Bureau Computer Incident Response Team (CIRT) or Bureau Privacy Officer (BPO)] records indicate that the following employee/contractor of [name of your organization] has committed a violation [or second violation, third violation, etc.] of a security regulation in safeguarding sensitive Personally Identifiable Information (PII) within [name of Bureau or Operating Unit]'s Information Technology system or facility.

[INSERT EMPLOYEE/CONTRACTOR'S NAME AND PII INCIDENT CASE # IN CAPS HERE]:

You are to remind the employee that:

- 1. A PII breach incident is considered a violation of a Department of Commerce (Department) security regulation;
- 2. Department employees/contractors have a responsibility to safeguard PII in accordance with Federal laws, regulations, and Department policies; and
- 3. Failure to adhere to these requirements may result in discipline or adverse action for Federal employees (oral admonishment up to removal from Federal service).

If you need additional guidance, please consult with [name of your servicing Employee Relations Specialist] at [telephone number and e-mail address].

The next level within your organization's management chain may be notified upon any subsequent PII breaches by this employee/contractor.

If you have any questions or need additional information about the PII incident, please contact me at [BPO contact information].

E-mail Notification to Next Level of Management/ Contracting Officer Representative at Subsequent Occurrences

[Insert Name of Bureau Computer Incident Response Team (CIRT) or Bureau Privacy Officer (BPO)] records indicate that the following employee/contractor of [name of your organization] has demonstrated [another violation, egregious disregard, or pattern of error] in safeguarding sensitive Personally Identifiable Information (PII) within [name of Bureau or Operating Unit]'s Information Technology (IT) system or facility.

[INSERT NAME OF EMPLOYEE/CONTRACTOR AND PII INCIDENT CASE # IN CAPS HERE]

On [insert date], the employee's supervisor/Contracting Officer Representative (COR) [insert name of employee's supervisor/COR] received notification of the employee/contractor's violation, was asked to take appropriate action, and was reminded of the following:

- 1. A PII breach incident is considered a violation of a Department of Commerce (Department) security regulation;
- 2. Department employees/contractors have a responsibility to safeguard PII in accordance with Federal laws, regulations, and Department policies;
- 3. Failure to adhere to these requirements may result in discipline or adverse action for Federal employees (oral admonishment up to removal from Federal service);
- 4. He/she should consult with [name], the servicing Employee Relations Specialist at [telephone and e-mail address] if additional guidance was needed; or [name], the COR if the individual is a contractor; and
- 5. The next level within his/her organization's management chain may be notified of any subsequent PII breaches by this employee/contractor.

The Department's Chief Privacy Officer (CPO) requests your assistance with ensuring additional appropriate action be taken to ensure this employee/contractor understands the importance of properly safeguarding sensitive PII Department Information Technology (IT) systems/facilities and does not continue to violate Department security regulations on safeguarding sensitive PII.

If you have any questions or need additional information, please contact me at [BPO contact information].