G A O
Accountability * Integrity * Reliability

Comptroller General
of the United States

United States Government Accountability Office
Washington, DC 20548

Decision

Matter of: Nuclear Regulatory Commission—Availability of Appropriations for Credit Monitoring Services

File: B-310865

Date: April 14, 2008

DIGEST

If the Nuclear Regulatory Commission were to mistakenly disclose to the public personally identifiable information of an employee or private citizen, its appropriation is available to pay for credit monitoring services as long as the Commission determines that it is necessary under the particular circumstances. In making such a determination, the Commission should be guided by the risk-based, tailored approach outlined by the Office of Management and Budget. Such an expenditure would be consistent with statutory breach notification and mitigation requirements and, notwithstanding any collateral personal benefit to an employee or individual, would be a necessary expense of the agency.

DECISION

The Nuclear Regulatory Commission (NRC) asks whether it may use appropriated funds to pay for credit monitoring services for employees or private citizens in the unlikely event that the government mistakenly discloses their personally identifiable information to the public. Letter from Leslie W. Barnett, Director, Division of Planning, Budget, and Analysis, Office of the Chief Financial Officer, NRC, to Gary L. Kepplinger, General Counsel, GAO, Dec. 4, 2007 (Request Letter). As discussed below, because NRC's appropriation is available for such a purpose as part of its overall information security program, we conclude that the expense would be authorized as a necessary expense of the agency, provided that the agency determines the expenditure to be necessary under the particular circumstances presented.[1]

[1] Our practice when rendering decisions is to obtain a factual record from the relevant federal agency and, as appropriate, other interested parties, and to elicit the legal position, if any, of the agency and other interested parties on the subject matter

(continued...)

In response to a request by the U.S. Customs and Border Protection on whether its appropriation is available to pay for credit monitoring services for employees who had become, or may become, victims of identity theft, we recently issued a decision stating that credit monitoring services for federal employees are generally personal expenses not chargeable to an agency's appropriation. B-309604, Oct. 10, 2007. The facts here lead us to a different outcome. Because the proposed purchase of credit monitoring services relates to a breach caused by the government and may be a means of mitigating damage resulting from the breach, appropriated funds are available for this purpose. In determining whether providing credit monitoring services is warranted in a particular situation, the agency should conduct a risk assessment and fashion a tailored response to the breach, consistent with applicable Office of Management and Budget (OMB) guidance.

BACKGROUND

By statute, federal agencies are responsible for providing information security protections and complying with security standards and guidelines. Federal Information Security Management Act of 2002 (FISMA), 44 U.S.C. § 3544(a). OMB has stated in its implementing guidance that "[s]afeguarding personally identifiable information in the possession of the government and preventing its breach are essential to ensure the government retains the trust of the American public." Memorandum for the Heads of Executive Departments and Agencies, OMB, May 22, 2007, *available at* www.whitehouse.gov/omb/memoranda/fy2007/m07-16.pdf (last visited Mar. 28, 2008). Agencies must also develop and implement an information security program, which, among other things, must include "procedures for detecting, reporting, and responding to security incidents," including "mitigating risks associated with such incidents before substantial damage is done." 44 U.S.C. § 3544(b)(7).

OMB has issued guidance providing a "menu of steps for agencies to consider" in the event of a data breach so that the agency "may pursue a risk-based, tailored response." Memorandum for the Heads of Departments and Agencies, OMB, *Subject: Recommendations for Identity Theft Related Data Breach Notification*, Sept. 20,

---

(...continued)
of the request. GAO, *Procedures and Practices for Legal Decisions and Opinions*, GAO-06-1064SP (Washington, D.C.: Sept. 2006), *available at* www.gao.gov/legal/resources.html. In this instance, the request letter provided sufficient information for our decision.

2006, at attachment, at 1 (September Memorandum).[2] The guidance points out that the precise steps to take must be decided in light of the particular facts presented and that in deciding whether to offer credit monitoring services, "agencies should consider the seriousness of the risk of identity theft arising from the data breach." September Memorandum at 7. It describes credit monitoring as "a commercial service that can assist individuals in early detection of instances of identity theft, thereby allowing them to take steps to minimize the harm." *Id.* at 6. The guidance states further that a credit monitoring service typically "notifies individuals of changes that appear in their credit reports, such as creation of a new account or new inquiries to the file." *Id.*

NRC states that it has robust programs in place to comply with all applicable requirements and the OMB directives on protecting personal information of employees and private citizens in its possession. Request Letter, at 1. As part of its security program, NRC has prepared a breach notification policy providing that the agency will "consider steps that can be taken to mitigate further compromise of [personal information] and to mitigate any negative results from the breach. . . . In addition to containing the breach, appropriate countermeasures, such as monitoring system(s) for misuse of the [information] and patterns of suspicious behavior should be taken." *NRC Breach Notification Policy*, at 7, *available at* www.nrc.gov/site-help/privacy.html#personal (last visited Mar. 28, 2008).

NRC is of the opinion that appropriated funds may be used to pay for credit monitoring services when the government is the cause of the mistaken disclosure of an employee's or private citizen's personal information. Request Letter, at 1. It believes that paying for such services, perhaps for a period limited to 1 year, would be a reasonable and cost-effective means of mitigating the adverse consequences resulting from the government's mistaken disclosure of an employee's or private citizen's personal information. *Id.*

DISCUSSION

Ordinarily, credit monitoring services are personal expenses because the expenditure primarily benefits the individual or employee, not the agency. Appropriations are generally not available for the personal expenses of government employees. B-309604, Oct. 10, 2007. We have allowed exceptions to the general rule when a particular expenditure for an item that is ordinarily considered to be personal in nature primarily benefits the government, notwithstanding the collateral benefit to the employee. B-302993, June 25, 2004. We generally resolve whether an

[2] This OMB memorandum is available at www.whitehouse.gov/omb/memoranda/fy2006/task_force_theft_memo.pdf (last visited Mar. 28, 2008).

expense is personal or official by assessing the benefits to the agency and the basis for the expenditure.

Unlike our recent decision addressing the use of the Customs and Border Protection's appropriation to pay for employees' credit monitoring services, in which we found the credit monitoring services for employees to be personal in nature, the NRC request presupposes that government action or inaction compromised the individuals' identities. Under these circumstances, the government has an interest in ensuring the public trust in handling the vast amounts of personal information it maintains. Moreover, Congress has required agencies to protect this information and has imposed affirmative obligations on agencies to address breaches and mitigate risks when government action or inaction mistakenly compromises personal information. As stated above, FISMA specifically addresses the possibility of inadvertent disclosures of information and requires agencies to have procedures for detecting, reporting, and responding to security incidents, including mitigating risks before substantial damage is done. 44 U.S.C. § 3544(b)(7).

In light of these obligations and responsibilities, we think that NRC would have a reasonable basis for such an expenditure: purchase of credit monitoring services for affected individuals is a means of mitigating the risk caused by the agency's inadvertent disclosure. NRC's intention of purchasing credit monitoring services, consistent with OMB policy, directly relates to the FISMA's statutory requirement to minimize damage resulting from breaches and appears to be a reasonable implementation of this requirement.

CONCLUSION

Given this statutory and administrative framework, we would not object to the use of appropriated funds to purchase credit monitoring services in the event of a security breach if the agency administratively determines that the expense is necessary. Any such determination, of course, should be made in accordance with OMB policy cautioning against routinely providing for such services in the event of a data breach.

Gary L. Kepplinger
General Counsel