Francis, Lezlie

From: Nichols-Streck, Lisa
Sent: Monday, March 21, 2016 10:02 AM
To: Fowble, Elizabeth; Heilig, Christoph
Subject: FW: Message to BISG re: Cybersecurity Intrusion

I believe this is the first email from OPM to NRC regarding the OPM breaches.

Non Responsive

From: Loss, Lisa M [mailto:Lisa.Loss@opm.gov]
Sent: Friday, June 05, 2015 11:18 AM

Kerben, Valerie; William Sticklen <william.k.sticklen.civ@mail.mil>; Corwin, David A. <David.Corwin@opm.gov>; Dininger, Charles F. <Charles.Dininger@opm.gov>; Gilmore, Michael <Michael.Gilmore@opm.gov>; Hajkowski, Inta <Inta.Hajkowski@opm.gov>; Hunt, Bruce E. <BRUCE.HUNT@opm.gov>; Flora, Jeffrey C. <Jeffrey.Flora@opm.gov>; Montgomery, Jody L. <Jody.Montgomery@opm.gov>; Mahoney, Michael J <Mike.Mahoney@opm.gov>; Sherwin, Mark P <Mark.Sherwin@opm.gov>; Marosy, William L. <William.Marosy@opm.gov>; McNally, Matthew A. <Matthew.McNally@opm.gov>; Miller, Merton W. <Merton.Miller@opm.gov>; Rainey, Anthony H. <Anthony.Rainey@opm.gov>; Sedor, Brian M <Brian.Sedor@opm.gov>; Sholhead, John E. <John.Sholhead@opm.gov>; Vinroe, Joyce <Joyce.Vinroe@opm.gov>; Booser, Leo R. <Leo.Booser@opm.gov>; DeMarion, Michele <Michele.DeMarion@opm.gov>; Eckenrode, Jennifer L. <Jennifer.Eckenrode@opm.gov>; Eury, Laura J. <Laura.Eury@opm.gov>; Faller, Michael T. <Michael.Faller@opm.gov>; Flora, Jeffrey C. <Jeffrey.Flora@opm.gov>; Furman, Travis W. <Travis.Furman@opm.gov>; Gellner, Rebecca A. <Rebecca.Gellner@opm.gov>; Gengler, Lindsay J. <Lindsay.Gengler@opm.gov>; Giancoli, Thomas A. <Thomas.Giancoli@opm.gov>; Hughes, Mari E. <Mari.Hughes@opm.gov>; Isacco, Andrea D. <Andrea.Isacco@opm.gov>; Dustin, Jacklin E <Jacklin.Dustin@opm.gov>; Alleman, Lisa M. <Lisa.Alleman@opm.gov>; McGarvey, Anthony J. <Anthony.McGarvey@opm.gov>; Mcleod, Donna L <Donna.Mcleod@opm.gov>; Means, Carol A. <Carol.Means@opm.gov>; Miller, Timothy C. <Timothy.Miller@opm.gov>; Moore, Timothy C <Timothy.Moore@opm.gov>; Morehart, Carol A. <Carol.Morehart@opm.gov>; Neiderhiser, Patricia A <Patricia.Neiderhiser@opm.gov>; Northime, Kimberly R. <Kimberly.Northime@opm.gov>; Parkinson, N. Roy <N.Parkinson@opm.gov>; Paul, Tammy L <Tammy.Paul@opm.gov>; Phillips, Jennifer L <Jennifer.Phillips@opm.gov>; Prasnikar, Trisha J. <Trisha.Prasnikar@opm.gov>; Reckner, Jennie L. <Jennie.Reckner@opm.gov>; Rodemoyer, Patty L. <Patty.Rodemoyer@opm.gov>; Schooley, Stephen M <Stephen.Schooley@opm.gov>; Scott, Shalonda A. <Shalonda.Scott@opm.gov>; Springer, Michele <Michele.Springer@opm.gov>; Waiter, Paul B. <Paul.Waiter@opm.gov>; Weber, Lynnette M. <Lynnette.Weber@opm.gov>; Wells, Jenny L. <Jenny.Wells@opm.gov>
Subject: Message to BISG re: Cybersecurity Intrusion

BISG Members,
Please be aware of the following information, which is also posted to the OPM website, www.opm.gov

Information About the Recent Cybersecurity Incident
June 4, 2015
The U.S. Office of Personnel Management (OPM) recently became aware of a cybersecurity incident affecting its systems and data that may have compromised the personal information of current and former Federal employees.

Within the last year, OPM has undertaken an aggressive effort to update its cybersecurity posture, adding numerous tools and capabilities to its networks. As a result, in April 2015, OPM became aware of the incident affecting its information technology (IT) systems and data that predated the adoption of these security controls.

Since the incident was identified, OPM has partnered with the U.S. Department of Homeland Security's U.S. Computer Emergency Readiness Team (US-CERT), and the Federal Bureau of Investigation to determine the impact to Federal personnel. And OPM immediately implemented additional security measures to protect the sensitive information it manages.

Beginning June 8 and continuing through June 19, OPM will be sending notifications to approximately 4 million individuals whose Personally Identifiable Information was potentially compromised in this incident. The email will come from opmcio@csid.com and it will contain information regarding credit monitoring and identity theft protection services being provided to those Federal employees impacted by the data breach. In the event OPM does not have an email address for the individual on file, a standard letter will be sent via the U.S. Postal Service.

In order to mitigate the risk of fraud and identity theft, OPM is offering affected individuals credit monitoring services and identity theft insurance with CSID, a company that specializes in identity theft protection and fraud resolution. This comprehensive, 18-month membership includes credit report access, credit monitoring, identity theft insurance, and recovery services and is available immediately at no cost to affected individuals identified by OPM.

Additional information is available beginning at 8 a.m. CST on June 8, 2015 on the company's website, www.csid.com/opm (external link), and by calling toll-free 844-222-2743 (International callers: call collect 512-327-0700).

Steps for Monitoring Your Identity and Financial Information

- Monitor financial account statements and immediately report any suspicious or unusual activity to financial institutions.
- Request a free credit report at www.AnnualCreditReport.com (external link) or by calling 1-877-322-8228. Consumers are entitled by law to one free credit report per year from each of the three major credit bureaus – Equifax®, Experian®, and TransUnion® – for a total of three reports every year. Contact information for the credit bureaus can be found on the Federal Trade Commission (FTC) website, www.ftc.gov (external link).
- Review resources provided on the FTC identity theft website, www.identitytheft.gov (external link). The FTC maintains a variety of consumer publications providing comprehensive information on computer intrusions and identity theft.
- You may place a fraud alert on your credit file to let creditors know to contact you before opening a new account in your name. Simply call TransUnion® at 1-800-680-7289 to place this alert. TransUnion® will then notify the other two credit bureaus on your behalf.

Precautions to Help You Avoid Becoming a Victim

- Be suspicious of unsolicited phone calls, visits, or email messages from individuals asking about you, your employees, your colleagues or any other internal information. If an unknown individual claims to be from a legitimate organization, try to verify his or her identity directly with the company.
- Do not provide personal information or information about your organization, including its structure or networks, unless you are certain of a person's authority to have the information.
- Do not reveal personal or financial information in email, and do not respond to email solicitations for this information. This includes following links sent in email.
- Do not send sensitive information over the Internet before checking a website's security (for more information, see Protecting Your Privacy, www.us-cert.gov/ncas/tips/ST04-013 (external link)).
- Pay attention to the URL of a website. Malicious websites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain (e.g., .com vs. .net).
- If you are unsure whether an email request is legitimate, try to verify it by contacting the company directly. Do not use contact information provided on a website connected to the request; instead, check previous statements for contact information. Information about known phishing attacks is also available online from groups such as the Anti-Phishing Working Group (www.antiphishing.org (external link)).
- Install and maintain anti-virus software, firewalls, and email filters to reduce some of this traffic (for more information, see Understanding Firewalls, www.us-cert.gov/ncas/tips/ST04-004 (external link); Understanding Anti-Virus Software, www.us-cert.gov/ncas/tips/ST04-005 (external link); and Reducing Spam, http://www.us-cert.gov/ncas/tips/ST04-007 (external link)).
- Take advantage of any anti-phishing features offered by your email client and web browser.
- Employees should take steps to monitor their personally identifiable information and report any suspected instances of identity theft to the FBI's Internet Crime Complaint Center at www.ic3.gov (external link).
- Additional information about preventative steps by consulting the Federal Trade Commission's website, www.identitytheft.gov (external link). The FTC also encourages those who discover that their information has been misused to file a complaint with the commission using the contact information below.

Identity Theft Clearinghouse
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
www.identitytheft.gov (external link)
1-877-IDTHEFT (438-4338)
TDD: 1-202-326-2502