Frequently Asked Questions

OPM Data Breach

Department of the Navy

26 June 2015
(*Information Included on Two Incidents*)

Table of Contents

Summary 2

Notification Update 3

General Information 5

What's Next 7

Appendix A - Guidance for Federal Employees and Retirees: 12

Appendix B - DONCEAP Identity Theft Information: 13

Note: As the OPM Data Breach is under federal investigation, this is an ongoing document that will continue to be updated as more information becomes available. ***This latest version identifies responses specific to the incidents reported by OPM.*** *Current FAQs also may be found at www.opm.gov.*

Summary – Updated

In April 2015, the Office of Personnel Management (OPM) became aware of a cybersecurity incident affecting its systems and data that may have compromised the personal information of current and former federal employees. The breach pre-dates OPM's adoption of tougher security controls. (Incident #1)

Since the incident was identified, OPM has partnered with the U.S. Department of Homeland Security U.S. Computer Emergency Readiness Team (US-CERT), and the Federal Bureau of Investigation to determine the impact to current and former federal employees. OPM estimates that up to 4 million employees may have been impacted by this breach.

OPM began conducting notifications to affected individuals using email and/or USPS First Class mail on June 8, 2015. Recognizing the inherent security concerns in this methodology, with OPM and CSID support, DoD suspended notifications to employees on June 11, 2015, until an improved, more secure notification and response process is in place. Late June 15, 2015, OPM advised that email notification resumed. Email notifications are still ongoing. U.S. Postal mail notifications will take longer.

OPM will offer impacted individuals 18 months of credit monitoring services and identity theft insurance through CSID – a company that specializes in identity theft protection and fraud resolution. The 18-month CSID membership will be offered to those individuals identified by OPM at no cost.

In the course of the ongoing investigation into the cyber intrusion that compromised personnel records of current and former federal employees (announced June 4), it was discovered that additional OPM systems were compromised. These systems contain information related to background investigations. OPM, the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI) are working as part of an ongoing investigation to determine the number of people affected by this separate intrusion. OPM will notify those individuals whose information may have been compromised as soon as practicable. (Incident #2)

Since the investigation is on-going, additional exposures may come to light; if this occurs, OPM will conduct additional notifications as necessary.

During the week of June 20, some employees began receiving an informational email with the subject line, "Update #2 for DoD Personnel on OPM Breach Notification Procedures." This is the first email that was sent to employees; therefore, employees should not "look" for email #1.

Notification Update

1. **Q: How will I be notified if I am an affected individual?**
   A: Incident #1 – OPM began conducting notifications to affected individuals using email and/or USPS First Class mail on June 8, 2015. Recognizing the inherent security concerns in this methodology, DoD, with OPM and CSID support, suspended notifications to employees between June 11-15, until an improved, more secure notification and response process is in place. Late June 15, 2015, OPM advised that email notification resumed.

   A: Incident #2 – The investigation into the second incident is ongoing. OPM will notify affected individuals as soon as practicable – keeping in mind that the investigation into the second breach continues.

2. **What do I need to do when I get the email?**
   A: Incident #1 – The email text now advises employees to paste or type a link to an https site. CSID also has changed the form on their initial page and only requires an employee to enter the unique PIN#. Additionally, employees will be asked to solve a CAPTCHA to help CSID block automated cyber attack programs. Once the PIN# and CAPTCHA are accepted, employees can proceed to the credit monitoring signup page – this is where personal information must be entered.

   Employees who have received a notification via email from the email account OPMcio@csid.com (or via letter from U.S. Postal Service) and entered their assigned PIN, are registered for the credit monitoring services.

   Affected employees who disregarded that email or deleted the email or affected employees who have not yet received the email will *automatically* be enrolled in the identity theft insurance. These employees will be re-notified by email with a PIN#.

3. **What happens if I didn't activate my PIN#?**
   A: Incident #1 – Employees who were notified by email **before** June 15 **and** who did **not** activate their PIN#, will be **re-notified** by another email**.**

4. **Q: Where will/did employees receive the email notification?**
   A: Incident #1 – Current federal employees who were affected should receive email notification using their work email. Some employees have indicated that the email notification went to their junk mail. It is strongly recommended that employees FIRST check their junk mail for OPM's email notification. The email notification should come from OPMcio@csid.com.

5. **Q: Will I receive notification by U.S. Postal mail if I don't receive an email notification?**
   A: Incident #1 – Employees will not receive notification by U. S. Postal mail unless employees do not have a work email address or if the email was rejected. If no notification is received, employees may call the CSID toll free number 1-844-777-2743 to authenticate their

status and receive their PIN#. Please expect long wait time, after listening to the recorded message, before reaching a customer service representative.

6. **Q: I've left federal service. How will I be notified if I have been impacted?**
   A: Incident #1 – If you have left the government, OPM will send you a notification via postal mail to the last address the agency has on file. OPM will verify this address with the National Change of Address (NCOA) service before mailing a letter.

7. **Q: I recently switched from one federal agency to another. How will I be notified if I have been impacted?**
   A: Incident #1 – If you have moved between agencies, OPM will send an email notification to your government email account for the agency at which you are currently employed. If your email address is unavailable, notification will be sent via postal mail.

8. **Q: I can't access the CSID website?**
   A: Incident #1 – As this is an evolving situation, there may be intermittent connectivity issues with the website. There also may be issues with volume and the large numbers of people trying to access the site. DoD CIO has asked Components to avoid blocking the CSID.COM/OPM website.

9. **Q: I have enrolled with CSID - why can't I login to my account?**
   A: Incident #1 – The web address for enrolling is https://www.CSID.com/OPM -- this site is for employees to set up accounts. Once you have enrolled, to login at a later time, go to https://opm.csid.com.

10. **Q: I received an email from opmcio@csid.com. Is this email from OPM, or is this a phishing message?**
    A: Incident #1 – The sender "OPM CIO" and email address "opmcio@csid.com" are the sender and email address that OPM is using to notify affected individuals. If you get an email about the breach from a different address, it is spam. Do not click on any links or provide any personal information. Contact privacy or security officers or follow Command or USMC protocols if receiving a suspected phishing message.

11. **Q: I believe I may have deleted the email notification. What do I do now?**
    A1: Follow these steps to attempt to retrieve the email:
    1. Open Outlook
    2. Click on "Deleted Items" Folder - on the left menu bar.
    3. On the very top of the page click "FOLDER" then --> Click the icon that says "Recover Deleted Items"
    5. Go through the list and select (mouse click on them) the ones to recover
    6. Navigate to the top of the screen and click the second icon on the top left (says "Recover Selected Items")
    7. This will recover the deleted email and return the email to the "Deleted Items" outlook folder

8. Simply move the email to your inbox

A2: Incident #1 – Call CSID at 1-844-777-2743 and they will authenticate your status as an impacted government employee and reissue your PIN on the phone. The employee will then use the PIN to register at the CSID website.

General Information

12. Q: When did this happen?

A: Incident #1 – OPM believes that the intrusion occurred in December 2014. OPM became aware of the intrusion into its systems in April 2015 after implementing tough new measures to deter and detect cyberattacks.

A: Incident #2 – During its investigation, OPM became aware of intrusions into its systems in May (affecting background investigations data). On June 8, 2015, OPM alerted agencies that there was a high degree of confidence that OPM systems containing information related to the background investigations of current, former and prospective federal government employees **and** those for whom a federal background investigation was conducted, *may have been* compromised.

13. Q: What personal information was compromised?

A: Incident #1 – OPM maintains personnel records for the federal workforce. The kind of data that may have been compromised in this incident could include name, Social Security Number, date and place of birth, and current and former addresses. It is the type of information you would typically find in a personnel file, such as job assignments, training records, and benefit selection decisions. OPM has indicated that it does not appear that names of family members, beneficiaries or information contained in actual policies were compromised. Please note, however, that DoD and DON employees and retirees may have had their information included in the human resources information that was compromised. The OPM notification will indicate what information may have been compromised.

Incident #2 – In the course of the ongoing investigation into the cyber intrusion that compromised personnel records of current and former Federal employees (announced June 4), it was discovered that additional OPM systems were compromised. These systems contain information related to background investigations. OPM, the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI) are working as part of an ongoing investigation to determine the number of people affected by this separate intrusion. OPM will notify those individuals whose information may have been compromised as soon as practicable.

14. Q: Why didn't OPM tell affected individuals about the loss of the data sooner?

A: Incident #1 – OPM became aware of an intrusion in April 2015. OPM worked with the DHS Computer Emergency Readiness Team (US-CERT) as quickly as possible to assess the extent of the malicious activity and to identify the records of individuals who may have been

compromised. During the investigation, OPM became aware of potentially compromised data in May 2015. With any such event, it takes time to conduct a thorough investigation and identify the affected individuals.

15. **Q: What systems were affected? Were DoD or DON systems affected?**
A: This incident impacts the OPM systems and data. Please note, however, that DoD and DON employees and retirees may have had their information included in the human resources information. For security reasons and due to the ongoing investigation, OPM cannot publicly discuss specifics that might be affected by the compromise of personnel data. OPM has added additional security controls to better protect overall networks and systems and the data they store and process.

16. **Q: Are TSP accounts impacted by the OPM cybersecurity incident?**
A: TSP account numbers are not shared with OPM and, as such, were not impacted.

17. **Q: Was other information compromised?**
A: Incident #2 – In the course of the ongoing investigation into this cyber intrusion, it was discovered that additional OPM systems were compromised. These systems contain information related to background investigations. OPM, the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI) are working as part of an ongoing investigation to determine the number of people affected by this separate intrusion. OPM will notify those individuals whose information may have been compromised as soon as practicable.

Who is Affected

18. **Q: How many individuals were impacted by the data breach?**
A: Incident #1 – OPM estimates about 4 million current and former employees may have had personally identifiable information (PII) compromised in the breach detected in April 2015. Since the investigation is ongoing, additional PII exposures may come to light. If OPM determines that more individuals have been impacted, they will conduct additional notifications.

Incident #2 – As the second incident investigation is ongoing, OPM will identify the breadth as soon as possible.

19. **Q: How many Department of Navy (DON) employees were affected?**
A: Currently that information is not available.

20. **Are retired civilians impacted by the data breach?**
A: Incident #1 – OPM continues to examine the data and systems that may have been compromised. For example, OPM has confirmed that any federal employee whose organization submitted records to OPM for future retirement process may have been

compromised – even if their full personnel file is not store on OPM's system. These individuals are included in the estimated 4 million individuals impacted by the first incident. Records that may have been compromised for these individuals may include service history records, court orders, and other records and information that pertain to annuity calculations. The PII data in these records includes name, Social Security numbers, and dates of birth as well as other information. Individuals who do not have a work email of record will be notified by U.S. Postal mail.

21. **Q: Were contractors affected by the breach?**
A: Incident #1 – Contractors were not affected unless they were previously a federal civilian employee.

Incident #2 – The investigation into the second incident is ongoing. Additional exposures may surface and, should that include contractors, OPM will conduct additional notifications.

22. **Q: Were current, retired or former military members affected?**
A: Incident #1 – OPM does not believe the first incident affected military records, unless they held a federal civilian position.

Incident #2 – The investigation into the second incident is ongoing. Additional exposures may surface and, should that include members of the military, OPM will conduct additional notifications.

23. **Q: How do we know that enrollment with CSID is secure and will not expose us to a second breach of our PII?**
A: CSID is an industry leader when it comes to identity theft protection and has a successful history of partnering with both public and private companies. Their company is embedded with security means to protect your information. CSID's site is scanned daily for thousands of hacker vulnerabilities and displays the McAfee SECURE trustmark.

What's Next

24. **Q: I received a letter stating that I have been affected. What should I do next?**
A: Please refer to the instructions in the letter or email. Many who have been notified have been advised to take advantage of the 18-month credit monitoring services and identity theft insurance through the company CSID. Impacted employees may also call 1-844-777-2743; (international callers can call collect at 512-327-0700) if they have questions. Due to a high volume of calls, employees may experience extended wait times. Typically, employees will not be able to register for the credit services by phone.

25. Q: Can I register by calling the CSID line?

A: No. After receiving notification, typically employees who have received the OPM notification must register online. However, employees can verify if they have been impacted by calling CSID at 1-844-777-2743. Please expect long wait times.

26. Q: What happens after I register?

A: Within about 24 hours after registering, employees will receive a subsequent email that advises the employee "Your CSID identity protection report is now available. One or more of your reports have been updated." Typically, the email follows by listing information which will be available to the employee to include:

- PayDay Loan - A PayDay Loan alert/report may include new inquires of new loans requested at a pay-day loan location using your identity;
- CyberAgentSM - A CyberAgentSM alert/report may contain matches for your information related to criminal chat rooms, news groups and other web sites where criminals trade or sell stolen identities;
- Court Records - A Court Records alert/report may contain matches for name and date of birth from county courts, Department of Corrections (DOC), Administration of the Courts (AOC), and other legal agencies. The types of offenses include felonies, misdemeanors, sexual offenses, traffic citations and more;
- Sex Offender - A Sex Offender alert/report may contain matches for your identity with in Sex Offender registry files or may be an update to registered Sex Offenders in your zip code;
- Social Security Trace - A Social Security Trace alert/report may lists addresses associated with your identity found in public records. A Social Security Trace alert/report may contain matches for your identity found in public records. If you have utilized a nick name in the past when applying for credit or you have changed your last name due to marriage, additional names may be reported. The email ends with a reminder to the employee to log in to their account at https://opm.CSID.com to view the details of this alert.

27. Q: What is OPM doing to prevent this kind of loss from happening again?

A: Because cyber threats are evolving and pervasive, OPM is continuously working to identify and mitigate threats when they occur. OPM evaluates its IT security protocols on a continuous basis to make sure that sensitive data is protected to the greatest extent possible, across all networks where OPM data resides—including those managed by government partners and contractors. More information on OPM actions are found at www.opm.gov.

28. Q: I did not receive a letter stating that my information was compromised, but feel that I should have. Can you help me?

A: Incident #1 – OPM has identified the individuals who have been impacted and began to notify individuals on June 8. They will continue to notify those who have been affected through the week of June 22.

Incident #2 – As the investigation is ongoing, additional individuals may be further identified and OPM will issue additional notifications as soon as practicable.

29. Q: Can my family members also receive services if they are part of my file/records?
A: Incident #1 – OPM has indicated that family members of employees were not affected by this breach. Therefore, they are not entitled to the credit monitoring and identity theft services provided by CSID through OPM.

Incident #2 – As the investigation into the breach of background information is ongoing, additional exposures may surface. OPM will conduct notifications as necessary.

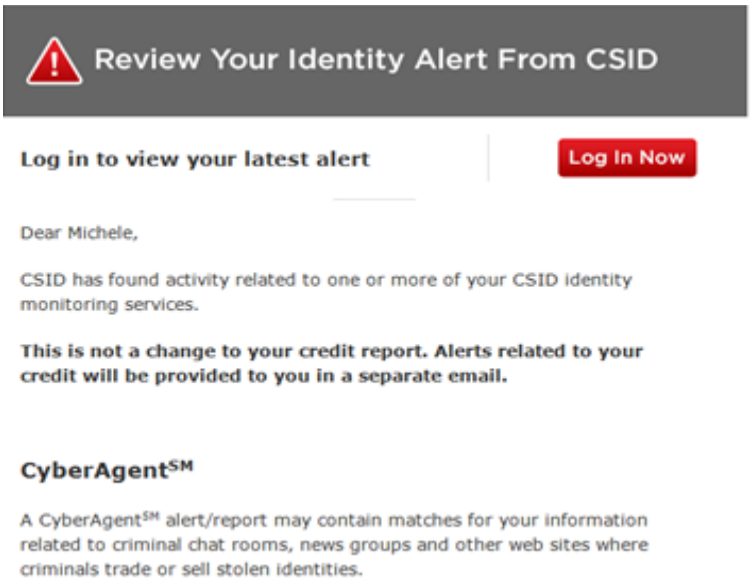
30. I received a notice for a family member who is deceased, what do I do?
A: Update contact information or the information about a deceased former employee by calling CSID's call center at 1-844-777-2743. If the notification was received by mail, OPM advises family members to destroy the letter and the mailer. No further action is required by the next of kin.

31. Q: Is it possible to decline CSID identity theft insurance?
A: Affected individuals are given complimentary identity theft insurance free of charge for 18 months. Every affected individual, regardless of whether or not they explicitly take action to enroll, will have up to $1 million of identity theft insurance and access to full-service identity restoration provided by CSID until December 7, 2016.

Participation in the credit monitoring services (a second step) is strictly voluntary on the part of the impacted employee.

32. Q: What if someone uses my identity to place unauthorized charges to my account?
A: Impacted individuals will have up to $1 million of identity theft insurance and access to full-service identity restoration provided by CSID which includes loss of income, child care, elderly care, unauthorized electronic funds transfer and legal costs. Impacted individuals who have enrolled and need to file a claim for fraudulent charges should call 1-844-777-2743.

33. Q: I received an email from CSID directing me to "review my identity alert". What is this? ***New***
A: If you receive this email, CSID has identified activity through their monitoring systems. This is not a change to your credit report. Alerts related to your credit will be provided to you in a separate email. You will be prompted to log in to your account to view the details of the activity via an alert (sample screen shot below on page 10).



Review Your Identity Alert From CSID

Log in to view your latest alert | Log In Now

Dear Michele,

CSID has found activity related to one or more of your CSID identity monitoring services.

This is not a change to your credit report. Alerts related to your credit will be provided to you in a separate email.

CyberAgent℠

A CyberAgent℠ alert/report may contain matches for your information related to criminal chat rooms, news groups and other web sites where criminals trade or sell stolen identities.

34. **Q: Can you confirm that the CSID monitoring program and insurance policy will not conflict with or adversely affect other protection I have with another company? I'd like to have both CSID and my current company monitor my accounts.**
    A: That is a question best addressed by credit professioals. While it may be unlikely that multiple credit monitoring services will adversely affect one another, it is not necessary (or recommended) that affected employees have two separate credit monitoring services.

35. **Q: Will my credit be impacted if I accept a credit report through the CSID monitoring program?**
    A: This is a government-sponsored service provided to affected employees and accepting the service will not, in and of itself, impact credit scores.

36. **How do I contact the CSID representatives?**
    A: Current and former federal employees can contact CSID between 7 a.m. and 10 p.m. CST, Monday through Friday, and 8 a.m. to 8 p.m., CST, on Saturdays, by calling the toll-free number 1-844-777-2743 (International callers may call collect at 512-327-0705). Highest call volume occurs between 9 a.m. and noon.

37. **Q: Do I need to notify my security office if I have detected fraudulent activity?**
    A: Employees should notify their security officer or supervisor in writing if fraudulent activity occurs.

38. Q: Does DON offer any services or information about identity theft?

A: The Department of the Navy Civilian Employee Assistance Program (DONCEAP) provides support for financial issues and identity theft for all DON civilians and their families. The 24/7 number is **1-844-DONCEAP** (1-844-366-2327) TTY 1-888-262-7848, International 001-866-829-0270. Information is also available at http://DONCEAP.foh.hhs.gov.

39. Q: I received a possible phishing message. Is this related to the breach? Who should I report the possible phishing?

A: If you believe you have received a possible phishing scheme, please report it to your CIO or security office as soon as possible. Employees may also send potential phishing messages to NMCI_SPAM@navy.mil

40. Q: I've noticed the identity theft protection provided by OPM is only available for 18 months. Will the CSID® coverage be extended beyond 18 months?

A: At present, OPM will provide the credit monitoring and theft identity services at no cost to impacted individuals for 18 months – the industry standard for identity theft protection. Impacted individuals will have up to $1 million of identity theft insurance and access to full-service identity restoration provided by CSID®. OPM will continue to assess and evaluate the need for additional measures should they be necessary.

41. Q: Is there anything else I can do?

A: OPM has provided guidance on safeguarding identity which is found in this FAQ document.

Appendix A - Guidance for Federal Employees and Retirees:

The following guidance is provided by OPM:

- Don't answer unsolicited phone calls, in-person visits or e-mails from anyone asking about federal employees or other internal information in your agency.
- Don't provide personal information or any information about your agency or how it's organized to anyone unless you know them or have verified that they're legitimate.
- Don't reveal your personal or financial information in e-mail — and don't follow links sent through e-mail.
- Do not send sensitive information over the Internet before checking a Web site's security.
- Pay attention to the URL of a Web site. Malicious Web sites 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're unsure whether an e-mail request is legitimate, try to verify it by contacting the sender directly. Don't use contact information provided on a Web site 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.
- Install and maintain anti-virus software, firewalls and e-mail 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 agency.
- Monitor your checking and other financial accounts, and immediately report any suspicious or unusual activity to your bank.
- Request a free credit report at www.AnnualCreditReport.com or by calling 1-877-322-8228. You're entitled by law to one free credit report per year from each of the three major credit bureaus. Contact information for the credit bureaus can be found on the Federal Trade Commission (FTC) Web site, www.ftc.gov.
- Review the FTC identity theft Web site, www.identitytheft.gov. The agency lists a variety of consumer publications that have a lot of information on computer intrusions and identity theft.
- Consider placing 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.

Appendix B - DONCEAP Identity Theft Information:

The following information is provided as a service by DONCEAP.

Are you a victim of ID Theft?

Has something like this happened to you?

- You get a phone call or letter telling you that you have been approved or denied credit for accounts that you never opened.
- You no longer receive your credit card statements, or you notice that some of your mail seems to be missing.
- Your credit card statement includes charges for things you know you never purchased.
- A collection agency contacts you for an account you never opened.

It's possible you've become a victim of identity theft. If you suspect any improper or illegal activity is taking place, here are some recommended steps:

1. Order a copy of your credit report to see if any new accounts or credit inquiries show up. Virtually all of your credit information is in your credit report. If someone is opening accounts in your name, it should show up there. If you suspect you've been a victim of fraud (for example; you've had your mail stolen, lost your wallet, or been contacted by a collection agency for an account you've never heard of), you should contact the fraud department of each credit bureau. You are eligible for a free credit report sent via U.S. mail if you are a victim of fraud or ID Theft.

2. Contact the fraud departments of each of the three major credit bureaus and report that you think your identity has been stolen. Request that a "Fraud Alert" be placed on your file and that no new credit be granted without your approval.

3. Research the crime and file complaints. Contact each company where you think you might have been a victim. Talk to their security or fraud department and explain what has happened. Review your account with them for any incorrect charges or a change of address. If you find something is wrong, you may need to close the account. If you open any new accounts, ask the company to put passwords on the account.

4. File a police report. File a report with your local police or the police where the identity theft took place. Get a copy of the report in case the bank, credit card company, or others need proof of the crime later on. Also, make sure that the crime is reported under identity theft.

5. Keep a log of all conversations and activities. Make notes of everyone you speak with; ask for names, department names, phone extensions, and record the date you spoke to them. Don't throw these notes away. Keep all notes and letters together in case they are needed in the future. Keep track of the time you spend documenting this information and lost hours at

work. You will need this information if the perpetrator is ever caught. You can be reimbursed for the time spent and hours lost.

6. File a complaint with the Federal Trade Commission (FTC). The FTC is the federal clearinghouse for complaints by victims of identity theft. Although the FTC does not have the authority to bring criminal cases, the Commission assists victims of identity theft by providing them with information to help them resolve the financial and other problems that can result from identity theft. The FTC also may refer victim complaints to other appropriate government agencies and private organizations for further action. If you're a victim of identity theft, you can file a complaint with the FTC by contacting their hotline.

   By phone: Toll-free 1-877-ID-THEFT (438-4338)
   Online: https://www.ftccomplaintassistant.gov/#crnt&panel1-1

7. Call the Social Security Administration if you suspect that your Social Security number is being fraudulently used.

   By phone: Toll-free 1-800-269-0271
   Online: www.ssa.gov

8. Contact the Internal Revenue Service if you suspect the improper use of identification information in connection with tax violations.

   By phone: Toll-free 1-800-908-4490
   Online: http://www.irs.gov/Individuals/Identity-Protection

9. For additional information on identity theft, including steps you can take to protect yourself from identity theft, or for assistance from DONCEAP's highly trained Fraud Resolution Specialists, civilian employees can contact DONCEAP 24 hours a day at 1-844-DONCEAP (1-844-366-2327) / (TTY: 1-888-262-7848) / International: 001-866-829-0270 or at DONCEAP.foh.hhs.gov.