QUESTIONS SUBMITTED BY EMPLOYEE GROUPS:

1) **When the website goes live on Monday, will employees be able to sign up for credit monitoring right away or do they have to wait for the email notification and/or letter via the U.S. Postal Service?**
2) **How do individuals enroll in the OPM-provided CSID services? Or must they wait for this info in the mailed notification?**

Questions #1 and #2 appear similar.
UPDATED Response: A PIN code will be provided by email/letter. Personnel will need this PIN code to register for the credit monitoring. If an individual has not received an email or letter yet but wishes to inquire, they may call the CSID call center. If an individual provides certain information to CSID, CSID will be able to provide the person's PIN if the person calls the call center. The PIN will help an individual access the CSID website which will provide information on whether the employee has been impacted and information for registering for the identify theft coverage. Individuals may contact the CSID call center by calling toll-free 844-222-2743 (International callers: call collect 512-327-0700).

3) **Are family members of current or former feds impacted by this breach?**

UPDATED Response: No. Family members are not impacted, but we also want to advise you that the investigation is ongoing. We will share additional information if and when we have it.

4) **Is there something they can tell employees to look for in the individual notifications to ensure they are legitimate? Especially in email communications? Anything we can tell them they will NOT be asked to provide, for example?**

UPDATED Response: Emails will be sent from opmcio@cisd.com. Neither OPM, nor any representative of OPM will initiate contact and ask for personally identifiable information, such as SSN, date of birth, or place of birth. Otherwise, you may contact the CSID call center for assistance by calling toll-free 844-222-2743 (International callers: call collect 512-327-0700).

5) **The school year for DoD teachers is over next week on June 12. Many overseas teachers will be traveling back to the United States for summer break and will not have access to their work email addresses. During the school year, they use APO/FPO addresses but many will be here stateside soon. How will DoD teachers be notified? The timing of the emails and / or letters may be problematic.**

RESPONSE*:* OPM is working with DoD and DoDEA to provide information in order to attempt notification this week before the school year ends on Friday, June 12th. However, an individual can also contact CSID by calling toll-free 844-222-2743 (International callers: call collect 512-327-0700). If an individual provides certain information to CSID, CSID will be able to provide the person's PIN if the person calls the call center. The PIN will help an individual access the CSID website which will provide information on whether the employee has been impacted and information for registering for the identify theft coverage.

6) **Was the central personnel data file breached?**
7) **Which system/systems were compromised? What specific types of my PII was stolen?**

Questions #6 and #7 appear similar.

Response: We are not identifying specific data bases impacted. 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 address. The communication to potentially affected individuals will state exactly what information may have been compromised.

8) **What will be done to reach employees who have email addresses but do not check email as a regular part of their duties? I think DECA, NAF, and wage grade employees would fall into this category but I am sure there are others. (rec'd 06/05/2015)**

RESPONSE: We encourage employees with email addresses to make an extra effort to check their work emails over the next two weeks, if at all possible. We appreciate any assistance the unions and management associations can provide to help spread the word. A PIN code will be transmitted either by email or letter to affected individuals between now and June 19th. However, an individual can contact CSID by calling toll-free 844-222-2743 (International callers: call collect 512-327-0700). If an individual provides certain information to CSID, CSID will be able to provide the person's PIN if the person calls the call center. The PIN will help an individual access the CSID website which will provide information on whether the employee has been impacted and information for registering for the identify theft coverage.

9) **If an employee is identified by OPM but for some reason does not receive notice (doesn't check their email, hasn't updated their mailing address), will they be able to check their status by contacting OPM? (rec'd 06/05/2015)**

RESPONSE: We encourage employees with email addresses to make an extra effort to check their work emails over the next two weeks, if at all possible. We appreciate any assistance the unions and management associations can provide to help spread the word. A PIN code will be transmitted either by email or letter to affected individuals between now and June 19th. (The following, struck through language, was found to be incorrect by FMA. We will correct this information once OPM has straightened the process out.)~~However, an individual can contact CSID by calling toll-free 844-222-2743 (International callers: call collect 512-327-0700). If an individual provides certain information to CSID, CSID will be able to provide the person's PIN if the person calls the call center.~~ The PIN will help an individual access the CSID website which will provide information on whether the employee has been impacted and information for registering for the identify theft coverage.

10) **Has contract employee PII been lost in addition to Federal employee PII? If so, how many impacted?**

Response: This is an on-going investigation. Based on what we know to date, the cyber incident impacts current federal civil service employees, retired civil service federal employees, and separated civil service federal employees.

11) **Will the Gov't consider providing lifetime credit protection for its work force as a new benefit to help retain and attract 21st century employees with modern protection needs? Think of it as the new health insurance. 5 years at a minimum!**

Response: 18 months of coverage is considered industry practice for this type of incident. However, since this is an on-going investigation, the government is evaluating how to provide employees with these types of protections in the most effective and cost efficient way.

OPM is providing comprehensive, 18-month membership for credit monitoring services and identity theft insurance through CSID, a company that specializes in identity theft protection and fraud resolution. All potentially affected individuals will receive a complimentary subscription to CSID Protector Plus for 18 months. Every affected individual, regardless of whether or not they explicitly take action to enroll, will have $1 million of identity theft insurance and access to full-service identity restoration provided by CSID.