SAND2015-7574C

Exceptional service in the national interest

Sandia National Laboratories

Office of Personnel Management Breach

Claudette Connor

Safeguards & Security Coordinator

Center 2500

U.S. DEPARTMENT OF ENERGY

NNSA National Nuclear Security Administration

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

OPM Cybersecurity Incidents

Personnel Records Incident: OPM identified that the personally identifiable information (PII) of approximately 4 million current and former **Federal employees had been stolen**.

Background Investigations Records Incident: OPM has concluded with high confidence that sensitive information of 21.5 million Federal employees and **Contractors** was stolen from the background investigation databases.

Vulnerability

e-QIP: OPM identified vulnerability in the Electronic Questionnaires for Investigators Processing. The system was taken offline on June 25, 2015. Security enhancements have been implemented and e-QIP has been brought back online as of July 24, 2015.

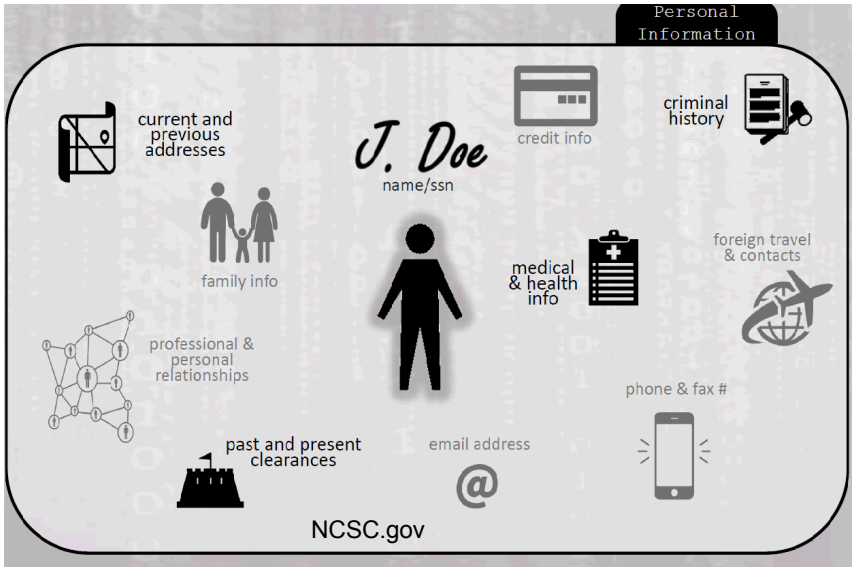
How does this affect me?

If you underwent an initial or reinvestigation in 2000 or afterwards, it is highly likely that you are impacted by the incident.

- 19.7 million individuals that applied for a background investigation, and 1.8 million non-applicants, primarily spouses or co-habitants of applicants were affected.

Notifications for this incident have not yet begun

Information Compromised



- Social Security Numbers
- Residency and educational history
- Employment history
- Information about immediate family and personal and business acquaintances

- Health, criminal and financial history
- Some records could also include:
  - Findings from interviews conducted by background investigators
  - Fingerprints
  - Usernames and passwords used to fill out your forms

Why You Might Be A Target

You could be targeted because you have information or are involved in activities of interest to foreign governments, criminals and extremists. Access to you can provide access to:

- Facilities
- Networks
- Personnel
- Sensitive information, intellectual property and controlled technologies

NCSC.gov

How It Happens

Sandia National Laboratories

How It Happens

Spearphishing

- Entice you into taking actions that could compromise computers or network
- Mislead you into opening a malicious attachment or link

Social Media

- Befriended via social media while posing as former acquaintance, job recruiter, etc. (eg, Facebook, LinkedIn)
- Collected information on you from social media postings

Human Targeting

- Meet you at venue of interest, reveal shared professions, interests, ideology, etc.
- Tests to see if you will wittingly or unwittingly provide information

NCSC.gov

Update August 6, 2015
Phishing Scams

TWO recent phishing attempts related to OPM breach:

Phishing occurs when a fraudster impersonates a business or a trusted individual in order to obtain private information.

- **The Federal Trade (FTC) Commission Phone SCAM**: Individuals are receiving a phone call from ***Dave Johnson*** claiming he is with the FTC in ***Las Vegas, NV.*** He claims he has money for victims of the cyber breaches.
  - FTC will never call and ask for PII, such as SSN or bank account numbers.
    - No Dave Johnson and No FTC office in Las Vegas, NV.
- **USAJOBS Phishing Scam:** OPM has provided warnings about email scams purporting to come from the Federal government's USAJOBS website.
  - The USAJOBS system will not send emails requesting that users validate account information.

➢ Employees should not click on links in these phishing attempts.

➢ They should not give out sensitive or personal information over the phone, internet, texts, or emails.

Protections Available

- Notice will be mailed in the coming weeks providing services available to Contractors, Spouses and Co-Habitants:
  - Full service identity restoration support and victim recovery assistance
  - Identity theft insurance
  - Identity monitoring for minor children
  - Continuous credit monitoring
  - Fraud monitoring services beyond credit files
  - You will be auto-enrolled in some services and will need to take action to enroll in others.
  - Services **will not** be provided to Immediate family or close contacts

What you should know…

- According to DOE Deputy Secretary

  "Victims of the recent breach **may face long-term and persistent counterintelligence vulnerabilities**."

- Acquisition of information may provide adversaries with the opportunity to target and collect additional information about or from employees and their relatives and associates.

- These attempts could include targeting via personal contact or through electronic devices such as smartphones and computers.

Guidance from DOE Office of Intelligence / Counterintelligence

- Be wary of attempted contact by individuals or groups unknown to you, whether by email, phone, social media, or personal encounters.
- Be attentive to transmission of personal and work-related information, particularly via phone and web. Encrypt sensitive information.
- Make an effort to understand and monitor your privacy and security settings on social media sites, especially those that reveal your geographic location, and adjust them accordingly.
- Talk with your immediate family members and share this same guidance. Ask them to tell you about any suspicious activities and contacts they experience.

DOE Office of Intelligence and Counterintelligence Guidance

- When traveling overseas, be particularly vigilant. You should assume that your affiliation with the U.S. Government is known to the foreign country you are visiting.
- If you are approached by anybody seeking sensitive information, please report that contact to the counterintelligence office or your supervisor when you can do so safely and securely.

What you can do

- Take advantage of all protection provided by OPM
- Visit IdentityTheft.gov to learn how to set up protections:
  - Get a free credit report
  - Set up fraud alerts on your accounts
  - Protect your children/minors from identity theft
  - Consider placing a credit freeze on your accounts
- Update your passwords
  - If you are using the same password that you did when you filled out your background investigation form, change them. Don't repeat passwords for several accounts.

Call to Action

Please report all suspicious activity to CI-Help@sandia.gov

For More Information

Sandia National Laboratories

- View the OPM website
- OPM Cyber Incidents https://powerpedia.energy.gov/wiki/OPM_Cyber_Incident
- Deputy Director Dan Payne, Counterintelligence and Security Center video https://www.youtube.com/watch?v=Vh_rAu3-Gb8&feature=youtu.be
- Email DOE cyber incidents with questions Call the DOE hotline at 855-719-4496 between 6 a.m.-10 p.m. EDT, Monday-Friday
- IdentityTheft.gov
- Members of the workforce should carefully consider **guidance** from the DOE Director of Intelligence and Counterintelligence regarding how to reduce vulnerability (Sandia Daily News, Monday, July 13, 2015).

UPDATE from OPM August 12, 2015

- OPM anticipates that the contract for identity monitoring and restoration services will be awarded in late August 2015, with notifications beginning soon thereafter.
  - OPM will provide updates on notification timing.
- Upon notification, individuals will also be able to sign up for services including identity and credit monitoring.