**Additional OPM Breach FAQs**

**Q: What happened?**

A: In June 2015, OPM discovered an additional 21.5 million individual’s personnel data had been compromised. OPM and an interagency team from the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI) have begun investigating the incidents. You may be affected if you underwent a background investigation through OPM in 2000 or years afterwards.

**Q: What is the e-QIP system?**

A: The Electronic Questionnaires for Investigations Processing (e-QIP) system is a web-based automated system that was designed to facilitate the processing of standard investigative forms used when conducting background investigations for Federal security, suitability, fitness and credentialing purposes. e-QIP allows the user to electronically enter, update and transmit their personal investigative data over a secure internet connection to a requesting agency.

Applicants can only access the e-QIP system if they have been invited to do so by an appropriate official at their sponsoring agency. Individuals cannot pre-apply for a security clearance, nor update their security questionnaire unless granted access by an appropriate agency official.

e-QIP was not compromised during the recent event; however, the government took this opportunity to strengthen all possible components of the system.

**Q: What has OPM done to strengthen the security of the e-QIP system?**

A: OPM is continuing to improve its defenses through their Information Technology (IT) systems by updating their authentication standards, continuous system monitoring, and hiring a new cybersecurity advisor.

**Q: Is there an alternative way to complete the clearance application outside of the e-QIP system?**

A: At this time e-QIP is the only method to complete a clearance application for this particular request.

**Q: What if I no longer wish to maintain my Security Clearance?**

A: Please consult with your Facility Security Officer and HR Business Partner to determine if you still require a Security Clearance.

**Q: What is Lockheed Martin doing for those that were recently impacted by the breach?**

A: While this was not a breach of Lockheed Martin systems, we are aggressively monitoring the incident and we will continue to provide updates. Lockheed Martin is offering U.S. domestic and expatriate employees three years of free identity protection services via Experian ProtectMyID. Additional information regarding identity protection can be found on [insideLM](https://insidelm.external.lmco.com/news-and-events/memo-lockheed-martin-offer-free-identity-protection).

**Q: What if I am the recipient of a spear-phishing email or a suspicious social networking attempt?**

A: Report any suspicious email activity or suspicious social networking attempts to the Lockheed Martin Computer Incident response Team (CIRT) and notify your Facility Security Officer.

**Q: What does Lockheed Martin do to ensure the protection of my Personal Information?**

A: LMSecurity is committed to protecting our employees’ sensitive information. We understand that the information you provide during the clearance process contains your Personally Identifiable Information (PII) and other highly sensitive information about your family and your personal life. We take this responsibility very seriously. We have implemented several measures intended to provide state of the art security protection for your sensitive information:

* We never share or disclose personal information to third parties.
* We utilize sophisticated software to encrypt your clearance application and signed releases at all times.
* Our digital fax solution immediately stores your fax encrypted at rest and at no time is your fax reduced to paper.

**Q: Where can I find additional information regarding the OPM/e-QIP cyber intrusion?**

A: More information and updates regarding the actions taken by OPM can be found on the [OPM Website](https://www.opm.gov/).

**Q: Where can I receive training for email awareness?**

A: As a Lockheed Martin employee, MyLearning offers an online course, “E-mail Awareness for Targeted Employees” (Course Code: 062744WPL02).

LMSOC-0986
REV: 07/29/2015