Timeline of Key Events [short version]

July 2012

- ✓ First known adversarial access to OPM’s network based on malware found in 2015.

Late 2013

- ✓ November: First evidence of adversarial activity associated with stolen technical documentation.

- ✓ December: First evidence of adversarial activity associated with background investigation and personnel records data breach. This activity was not identified until April 2015.

March 2014

- ✓ OPM notified of data breach identified by a third party. While OPM responds to this notice and monitors adversarial activity targeting background investigation data, adversary exfiltrates documents related to the OPM systems holding background investigation data.

- ✓ Witness involved in the 2014 and 2015 incident response efforts, said the material exfiltrated would give an attacker targeting the background investigation data an advantage because *“it gives them more familiarity with how the systems are architected. Potentially some of the documents may contain accounts, account names, or machines names, or IPT addresses that are relevant to these critical systems*.”

May 2014

- ✓ May 7 – adversary associated with exfiltrating background investigation data establishes a foothold on OPM’s network using OPM credentials for background investigation contractor.

- ✓ May 27 – OPM successfully executes a plan to expel the attacker they began monitoring in March 2014, but is unaware of and does not eliminate the May 7 foothold.

June 2014

- ✓ Adversary conducts a remote desktop protocol session contacting important and sensitive servers supporting…background investigation processes indicating escalated access and ability to move through OPM’s network.

- ✓ Adversary likely first had access to OPM’s mainframe.

July – August 2014

- ✓ After moving throughout OPM’s network and obtaining elevated access credentials, the adversary successfully exfiltrates the background investigation data from OPM’s network.

July 2014

- ✓ OPM acknowledges (in response to press reports) material was exfiltrated in 2014, but does not identify this material as related to background investigation systems and states no personally identifiable information exfiltrated.

December 2014

- ✓ After moving throughout OPM's network to the Department of Interior's data center holding OPM data, adversary exfiltrates personnel records data.

March 26, 2015

- ✓ Fingerprint data appears to have been exfiltrated on or around this date.

April 15, 2015

- ✓ After being alerted by an OPM contractor working for OPM's IT security operations group, OPM notifies US-CERT about suspicious network traffic related to opmsecurity.org. This domain was registered to Steve Rogers, a.k.a. "Captain America" in April 2014 and the last beaconing activity occurred in March 2015.

April 22, 2015

- ✓ Then-CIO Seymour testifies before the Committee on cybersecurity and publicly discusses the data breach of the materials exfiltrated in spring 2014 (related to background investigation systems) saying "..so in this case, potentially, our antiquated technologies may have us a little bit."

April 23, 2015

- ✓ OPM determines there was a major incident regarding the exfiltration of personnel records, which triggers a requirement to notify Congress. Congress notified April 30.

May 20, 2015

- ✓ OPM determines there was a major incident regarding the exfiltration of background investigation data, which triggers a requirement to notify Congress. Congress notified May 27.

June 2015

- ✓ June 4 – OPM releases public notice that personnel records of 4.2 million current and former federal employees had been compromised.

- ✓ June 16 – the Committee holds first of two hearings on the OPM data breaches.

July 9, 2015

- ✓ OPM releases public notice that background investigation data of over 20 million former and current federal employees and contractors had been compromised.