Nghia Hoang Pho

- National Security Agency (NSA) employee
- Held Top Secret/SCI clearance
- Employed as a developer in Tailored Access Operations (TAO) at the NSA
- Sentenced to 66 months in prison, followed by three years of supervised release

CDSE

Center for Development of Security Excellence

CASE STUDY

WILLFUL RETENTION OF CLASSIFIED NATIONAL DEFENSE INFORMATION

WHAT HAPPENED

Nghia Hoang Pho was employed as a developer in Tailored Access Operations (TAO) at the National Security Agency (NSA). NSA's TAO involved operations and intelligence collection from foreign automated information systems or networks, as well as actions taken to prevent, detect, and respond to unauthorized activity within DoD information systems and computer networks.

Pho received training regarding classified information, including the proper handling, marking, transportation, and storage of classified materials. He knew the unauthorized removal of classified materials and transportation and storage of those materials in unauthorized locations risked disclosure and transmission of those materials and therefore could endanger the national security of the United States and the safety of its citizens.

Beginning in 2010 and continuing through March 2015, Pho removed and retained U.S. Government property, including documents and writings that contained national defense information classified as Top Secret and Top Secret/SCI. Pho retained documents, in hard copy and digital form, containing national defense and classified information in a number of locations within his residence in Maryland.

The New York Times reported that the TAO developer brought home the materials so he could update his resume. At his sentencing hearing, Pho claimed he took copies of U.S. Government documents and writings containing national defense information so he could work from home. He said he was trying to earn a promotion as he neared retirement.

The case documents do not give much indication of what types of data and materials Pho took and left on his personal computer. The frantic investigation into valuable NSA tools that were stolen by Russian spies, though, indicates that Pho may have exposed more than just resume materials.

INDICATORS

- Access Attributes – Pho held a Top Secret/SCI clearance
- Foreign Considerations – Pho is believed to be the NSA employee from whom Russia stole valuable data by compromising the Kaspersky antivirus software.
- Security and Compliance Incidents – Despite his training, Pho took classified materials home and stored them in unauthorized locations.

IMPACT

- Moscow-based Kaspersky Labs has acknowledged copying Pho's secret files via antivirus software on his computer. Because antivirus software has deep and far-reaching permissions, Russian intelligence used its connections into the Kaspersky software to lift files, and any number of secrets. Kaspersky has repeatedly denied any association with the Russian government.
- "Pho's intentional, reckless and illegal retention of highly classified information over the course of almost five years placed at risk our intelligence community's capabilities and methods, rendering some of them unusable" – John C. Demers, Assistant Attorney General for National Security
- "Pho compromised some of our country's most closely held types of intelligence and forced the NSA to abandon important initiatives to protect itself and its operational capabilities at a great economic and operational cost" – Robert K. Hur, U.S. Attorney for the District of Maryland
- Despite his claim of an innocent motivation, Pho acted deliberately over a period of five years. And his removal of these sensitive materials forced the NSA to abandon years of signals collection work.
- "The fact that such a tremendous volume of highly classified, sophisticated collection tools was removed from secure space and left unprotected, especially in digital form on devices connected to the Internet, left the NSA with no choice but to abandon certain important initiatives, at great economic and operational cost," - NSA Director Admiral Mike Rogers wrote.

ADDITIONAL INFO

"The privilege of working for the U.S. Intelligence Community requires strict adherence to laws governing the lawful secrecy of its work," said Special Agent in Charge Gordon B. Johnson. "We cannot have a functioning Intelligence Community without the protection of sources and methods, and taking classified information and placing it in a vulnerable setting has profound and often disastrous consequences. This case is a clarion call to all security clearance holders to follow the law and policy regarding classified information storage. The FBI will leave no stone unturned to investigate those who compromise or mishandle classified information."

Resources for further exploration:

- Need-to-Know Principle
  https://www.cdse.edu/Training/Security-Training-Videos/Personnel/Need-to-Know-Principle/
- Classified Information Nondisclosure Agreement (SF-312)
  https://www.gsa.gov/cdnstatic/SF312-13.pdf?forceDownload=1
- Introduction to Information Security (IF011.16)
  https://www.cdse.edu/Training/eLearning/IF011/

IF YOU SEE SOMETHING, SAY SOMETHING!

Contact the appropriate POC to report any observed potential risk indicators:

Name_____ **Agency** _____

Title: Supervisor/Security Officer/ITP Senior Official/ITP Manager