The National Counterintelligence Executive

- Reports to the Director of National Intelligence; however, the NCIX’s authorities reach across the USG.

- The NCIX was created to serve as the head of national counterintelligence for the U.S. Government.

- The ONCIX mission includes carrying out and coordinating outreach programs, including to the US private sector.
Cyber Espionage

- Reports over the past decade estimate the loss from cyber espionage to be in the billions per year.

- Proliferation of CNO tools by foreign companies and the underground market gives *less capable* actors means to conduct cyber (*and supply chain*) attacks.

### WHERE IS THE THREAT COMING FROM?

<table>
<thead>
<tr>
<th>Date</th>
<th>Event Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>February 2013</td>
<td>Mandiant report exposed China’s cyber espionage capabilities with attribution.</td>
</tr>
<tr>
<td>May 2013</td>
<td>Intellectual Property Commission Report estimated China is responsible for 50% to 80% of international IP theft.</td>
</tr>
<tr>
<td>September 2013</td>
<td>Symantec Hidden Lynx report exposed East Asian hackers targeting supply chains using a custom driver application.</td>
</tr>
<tr>
<td>June 2014</td>
<td>Symantec Dragonfly report exposed East European hackers targeting suppliers for US and European energy companies.</td>
</tr>
</tbody>
</table>

**Who else?**
INFORMATION AND COMMUNICATIONS TECHNOLOGY (ICT) INDUSTRY A PRIME TARGET

(U) The ICT industry is a target:
Unless operations are for disruptive purposes, as we build robust and enduring cyber security into our networks, current and future supply chain operations must have a cyber component.

* Supply Chain Access Operations involve the modification of hardware or software with the purpose of enabling CNE.
USG Challenges and Successes

- Information Sharing
  - Good, bad, and ugly
- Volume, Volume, and Volume
  - Where are the Resources?
- Criticality Analysis
  - Both good and bad
- Supply Chain Views
  - Counterintelligence
  - Engineers
RISK MANAGEMENT

- 100% protection cannot be achieved, regardless of expenditures
- Risk Management is the foundation of Corporate Counterintelligence programs
Supply Chain Risks
CASE EXAMPLES

(U) East Asian Cyber Attacks on Supply – Hidden Lynx & TrapX

(U) East European Cyber Attack – Dragonfly

(U) Information Security Company #1

(U) Data Virtualization Company

(U) Information Security Company #2

(U) Information Security Company #3

(U) VOIP Company

(U) Speech Recognition Company
QUESTIONS