Welcome to Sandia’s Small Business Forum!

Our Topic Today: Securing Your Small Business Supply Chain
Agenda

- Welcome & Introduction – Eric Lochausen, Supplier Diversity Advocate
- Supply Chain Risk Management (SCRM) Overview – Paul Sedillo, Small Business Program Manager
- Presenters – Shannon Mulligan & Jason Maestas, Supply Chain Analysts
  - SCRM is where we are headed
  - Counterfeiting
  - Software
  - Cyber Espionage
  - Maturing your SCRM Program
- Final Remarks – Eric Lochausen, Supplier Diversity Advocate
Sandia National Laboratories Supply Chain Risk Management Team has trained and presented at the:

- Pentagon
- White House
- Department of Energy
- Department of Defense
- Various DOE National Laboratories
Our Goal for Today!

Offer guidance into how your supply chain can become more…

… so US national security can be strengthened!
Securing Your Small Business Supply Chain

Shannon Mulligan and Jason Maestas
“If the Covid-19 pandemic and resulting product shortages were not a sufficient wake-up call, the recent software supply chain attacks on U.S. industry and government should serve as a resounding call to action. We must enhance the **resilience, diversity, and security of our supply chains**. The vitality of our nation depends on it,”

- Michael Orlando, Acting NCSC Director
The globalization of the world economy has placed critical links in the manufacturing supply chain under the direct control of U.S. adversaries.

...not only do U.S. adversaries use access to the supply chain to pursue technologies and gain access to sensitive systems, foreign manufacturers can also, simply and effectively, insert counterfeit parts into products destined for the United States and degrade the performance of U.S. systems.—NCIX (Counterintelligence Executive)
Attack Space is infinite

Financial

Get Junk

Sell Junk

Make $$$

Deny
Delay
Disrupt
Discover

Hardware

Software

Information

DOE

DOE

DOE

me
me
me
me
me
me
me
me
me

U
U
U
U
U
U
U
U
U

s
s
s
Electronics counterfeiting

Source: ERAI, Inc INSIGHT Newsletter, Q4-2018
The Purpose of S/CI Awareness

- There is an increase in suspect/counterfeit products, along with cybersecurity risk
- The global impact of the Covid-19 Pandemic

How can S/CI affect your business as well as your personal life?
Define: SUSPECT

Suspect items
- May have been misrepresented

ART For use With in for.
information technology equipment
Made in China
Define: COUNTERFEIT

Counterfeit items
- found proof that item is misrepresented
Impact

- **Government:** Weapons, military equipment, aerospace, etc.
- **Industry:** Nuclear Power, Petrochemical, Commercial Aircraft (FAA), etc.
- **Consumer Products:** Bicycle parts, phones, electronics, electrical products, sporting equipment, handbags, shoes, food, medicine, pet supplies, etc.

Anything can be counterfeit!!
Impact

In 2014 estimated (IACC):

• $250 Billion in the US
• $1.77 Trillion worldwide

In 2016 a report from US Chamber of Commerce Global Intellectual Property Center:

• In 2012, DOD found 1,800 cases of suspected counterfeit parts
• Deaths related to counterfeit products is est. at $18 Billion worldwide
• Clear link between counterfeiting and terrorism
Work
Environment
Quality Products-
Services
Safety
NATIONAL SECURITY
Reputation

HOME
family
Beware of Counterfeiters in online marketplaces!

• Buy direct from the company.

• Most active in online marketplaces.

• Virtual flea markets.

• Increasingly greater numbers of consumers are using online marketplaces.
  • 2.14 billion digital buyers this year!*

• Avoid prices that are too good to be true
Vet third-party sellers

Just so you know…Creating a seller profile online is relatively easy

1. To start… click on the product from the results page.
2. Look for a List of other products the vendor is selling.
3. Don’t recognize the vendor? Google it and look for at least one of these:
   • A verifiable website information.
   • Authentic social medial presence
   • BBB or Glassdoor reviews.
   • Other recognizable retailers that carry the vendor’s products.
Look past the “Recommended” or “Choice” labels

• Many of the “Choice” recommended listings are:
  • Mislabeled
  • Unsafe
  • Banned products listings from third parties

• “Choice” is not a marker of safety, but is based on:
  • Price
  • Shipping speed
  • Reviews

• The first few products displayed are typically sponsored by vendors
Review the Reviews

• Fake reviews are rampant!

• Vendors and third party vendors are trying to game the review system

• What can you do?
  • Read through numerous reviews, not just the 5 stars.
  • Ensure language used in the review matches the product.
Beware of certain types of products

• Majority of consumer merchandise falls under the jurisdiction of the FDA or CPSC.

• Rebranding is an issue!

• Items that run a higher risk of being unsafe:
  • Products or accessories that touch your skin (especially ointments and makeup).
  • Masks, helmets, or anything that covers your face.
  • Products for children or babies.
  • Lithium-ion batteries or products that contain them.
  • Anything that plugs into the wall.
Still not sure? Buy it elsewhere.

- If becoming a detective before you purchase online seems like too much, look at brick-and-mortar stores or other websites.

- “Big box” retailer websites offer a safer experience
  - Both Target and Walmart good examples
• **Mimics** of popular websites

• **Domain age** is very new and may have been setup just to sell during the holidays or at peak times

• Poor grammar and spelling

• Lack of **contact information** or use of only generic entry forms for contact

• Payments are **unsecured**

• Deals that are too good to be true
OPSEC TIPS for ELECTRONIC DEVICES

- Be aware of what apps you are downloading
- Keep devices up to date
- Use multi-factor authentication
- Offer a “guest” WIFI network
- Don’t leave WIFI or Bluetooth on in public settings
Capacitors
EVEN YOU can inspect deliverables!

Nationally Recognized Test Laboratories

Different Pin Indicators in same lot?

Contamination and scratches on leads?
"ART" is not a genuine company

"CE" symbol looks to have been stamped over (CE is also not recognized as an NRTL mark in the US for electrical safety like UL or ETL)

"US TEO" should actually read "LISTED"

"With" is capitalized when normally it is not

Information is split instead of one continuous word

"E233466" is a UL number but this is not UL certified

Model# A1265 is associated with Apple phone chargers
Obsolescence prevention

Source selection (in order of priority):
- Original component manufacturers
- Franchised distributors
- Qualified Independent Distributor

Clearly State Procurement Requirements and Specifications
Prevention Guidance

➢ **Quality system audits and/or Counterfeit parts mitigation process audits**
  ◦ Equipment providers (e.g., AS9100)
  ◦ Distributors (e.g., AS9120)

➢ **Review the supplier's returns process (RMA) as applicable**
  ◦ A weak returns process is one way an otherwise good supplier (authorized or not) could be exposed and inadvertently pass on counterfeit components.
Things you might find and want to avoid…
There are many commercially available tools to report items:

- Contact the manufacturer and let them know you may have a counterfeit


- Report Intellectual Property Theft at the National Intellectual Property Rights Coordination Center at [www.ice.gov/pi/cornerstone/ipr](http://www.ice.gov/pi/cornerstone/ipr)
WHAT to do and WHO to contact regarding S/CI?

1. For questions or to report suspect or counterfeit items, materials, services, or software:
   - SNL Suspect/Counterfeit Items Program Coordinator: sqasci@sandia.gov
   - Do not use item
   - Do not throw item away

2. To report suspected fraud, waste, or abuse by a DOE employee, Subcontractor, or grant recipient involving DOE programs:
   - Office of Inspector General:
     - (800) 541-1625
     - ighotline@hq.doe.gov

Additional information: http://energy.gov/ig/office-inspector-general.

Report items, no matter the value or intended use if you suspect it may be counterfeit!
Other Resources


Federal Trade Commission: www.ftc.gov

US Chamber of Commerce Global Intellectual Property Center (GIPC) www.theglobalipcenter.com

International Trademark Association: www.inta.org

Government Industry Data Exchange Program (GIDEP): www.gidep.org
Software: Backdoors, Ransomware, Malware

Sources: “Foreign Economic Espionage in Cyberspace”, National Counterintelligence and Security Center, 2018
https://www.dni.gov/index.php/ncsc-home;
https://antivirus.comodo.com/blog/computer-safety/shadowpad-malware-strikes-netsarang-products/
Some Countries blocking outside software

Even YOU can practice SCRM for software

1. Use and update your antivirus software.

2. Before you download or purchase software:
   • National Vulnerability Database: https://nvd.nist.gov/vuln/search
   • Common Vulnerabilities and Exposures: http://cve.mitre.org/cve/search_cve_list.html

3. If you purchase custom software, ask lots of questions!
   ◦ Static and dynamic testing methods?
   ◦ Third Party or Open Source content?
   ◦ How are remote system maintenance or upgrades trustworthy?

Read the documentation to fully understand all the functions and features (ex. wireless features)
Cyber Espionage: Industries of Interest

WANTED BY THE FBI

HOSSEIN AHMAD LARIJANI
Conspiracy to Defraud the United States by Dishonest Means; Smuggling; Illegal Exports and Attempted Illegal Exports in Violation of the International Emergency Economic Powers Act (IEEPA); Obstruction of Justice

Photograph taken circa 2007

DESCRIPTION

<table>
<thead>
<tr>
<th>Aliases:</th>
<th>Hossein A. Larijani, Hossein Larijani</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date(s) of Birth Used:</td>
<td>October 31, 1963</td>
</tr>
<tr>
<td>Hair:</td>
<td>Black</td>
</tr>
<tr>
<td>Height:</td>
<td>Approximately 5’8”</td>
</tr>
<tr>
<td>Sex:</td>
<td>Male</td>
</tr>
<tr>
<td>Occupation:</td>
<td>Businessman</td>
</tr>
<tr>
<td>Languages:</td>
<td>Persian (Farsi), English</td>
</tr>
<tr>
<td>Place of Birth:</td>
<td>Tehran, Iran</td>
</tr>
<tr>
<td>Eyes:</td>
<td>Black</td>
</tr>
<tr>
<td>Weight:</td>
<td>Approximately 175 pounds</td>
</tr>
<tr>
<td>Race:</td>
<td>White</td>
</tr>
<tr>
<td>Nationality:</td>
<td>Iranian</td>
</tr>
<tr>
<td>NCIC:</td>
<td>W42164733</td>
</tr>
</tbody>
</table>

REWARD

The United States Department of State’s Transnational Organized Crime Rewards Program is offering a reward of up to $3 million for information leading to the arrest and/or conviction of Hossein Ahmad Larijani.

REMARKS

Source: ERAI, Inc INSIGHT Newsletter, Q4-2018 and www.fbi.gov
Russia

PyeongChang 2018

Even YOU can Practice Basic Cybersecurity!

Federal Trade Commission: https://www.ftc.gov/SmallBusiness
Even YOU can Practice Basic Cybersecurity!

Assessment & Auditing Resources

<table>
<thead>
<tr>
<th>General</th>
<th>Critical Infrastructure</th>
<th>SMB</th>
<th>International</th>
</tr>
</thead>
<tbody>
<tr>
<td>Federal</td>
<td>Assessment &amp; Auditing</td>
<td>SLTT</td>
<td>Academia</td>
</tr>
</tbody>
</table>

Resources relevant to organizations with regulating or regulated aspects.

- Axio Cybersecurity Program Assessment Tool
  (A free assessment tool that assists in identifying an organization’s cyber posture.)
- Baldridge Cybersecurity Excellence Builder
  (A self-assessment tool to help organizations better understand the effectiveness of their cybersecurity risk management efforts and identify improvement opportunities in the context of their overall organizational performance.)
- Cohesive Networks’ "Putting the NIST Cybersecurity Framework to Work"
  (A guide for using the NIST Framework to guide best practices for security audits, compliance, and communication.)
- Facility Cybersecurity Facility Cybersecurity Framework (FCF)
  (An assessment tool that follows the NIST Cybersecurity Framework and helps facility owners and managers manage their cyber security risks in core OT & IT controls.)
- FINISPECTECH’s Cybersecurity Framework as a Service
  (A user friendly Framework management tool.)
- Information Systems Audit and Control Association’s Implementing the NIST Cybersecurity Framework and Supplementary Toolkit
- ISACA’s Cybersecurity Based on the NIST Cybersecurity Framework
  (An audit program based on the NIST Cybersecurity Framework and covers sub-processes such as asset management, awareness training, data security, resource planning, recover planning and communications.)
- Rivial Security’s Vendor Cybersecurity Tool
  (A guide to using the Framework to assess vendor security.)
- University of Maryland Robert H. Smith School of Business Supply Chain Management Center’s CyberChain Portal-Based Assessment Tool
  (Provides guidelines to measure and assess cyber supply chain risk.)

https://www.nist.gov/cyberframework/assessment-auditing-resources
Maturing your SCRM practices

Know your suppliers
- Make/Buy Determinations
- Acquisition Planning
- Subcontractor Qualification
- Sourcing Decisions
- Contract Negotiations & Management
- Receipt & Inspection of Deliverables
- Subcontractor Performance Management

Enhance your SCRM Ts&Cs
- SOWs w/ all Quality Requirements

Know your suppliers

Relevant Policies and Potential Flow downs

- DFAR 252.204-7012 (Safeguarding Unclassified Controlled Technical Information)
- NAP-24A (Weapons)
- DOE O 414.1D (S/CI)
- NAP 14.1-D (NIST)
- DOE O 205.1B (SCRM/Cyber)
- DOE O 471.6 (Information Protection)
Modern SOWs: All Requirements and No Fluff!

**Requirements-Driven**
- Technical Quality
- Configuration Mgmt
- Reporting & Monitoring
- Acceptance Criteria
- Support & Maintenance
- Nonconformances
- Shipping
- Disposition of Excess Drawings

**Peripheral Project Info**
- Inspection methods
- Sampling or Test processes
- Criticalness
- Next assembly
- Other Interfaces
- BOM for project
- Other background program information, or members of Supply Chain
Information will be provided on a Need To Know Basis!

<table>
<thead>
<tr>
<th>Technical information</th>
<th>Project management information</th>
<th>Connections/Contacts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Potential and approved designs</td>
<td>Project information: Schedules, budgets, project details (ordering organization, WBS, project/task structure, project protection plans) Lessons learned: What is broken, where relationships or processes fail, where there are delays Waste and spare part determination Lifecycle processes or patterns Transportation details</td>
<td>Employment/partnership/conference interaction opportunities Leadership/personnel identification Potential and selected vendors/contractors Successes/awards</td>
</tr>
<tr>
<td>Production materials, components, technologies, and problems (including solutions)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Science and technology innovations</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
We Make Parts for Nuclear Weapons Here!

--Supplier X
Small Business can be BEST, lowest risk Sources

- No issues beneath the surface
- Cybersecurity and SCRM practices easier to upgrade
- Agility for reporting and reacting
Thank you!

If you have a question, email it to supplier@sandia.gov. Questions will be collected from 10/12/21 through 10/22/21.

Questions and answers will be emailed to participants in November.