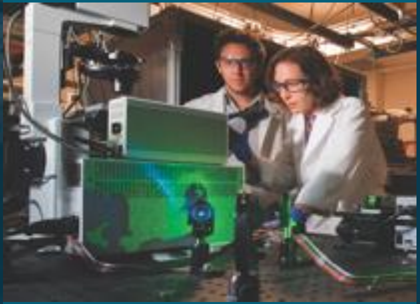
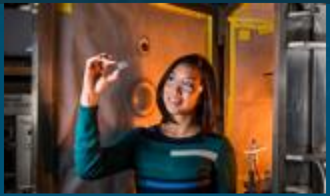
Supply Chain Risk Management & Small Business





PRESENTED BY

Amber Romero, C.P.M., PMP

Sandia National Laboratories, Albuquerque, NM

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

Today's topics

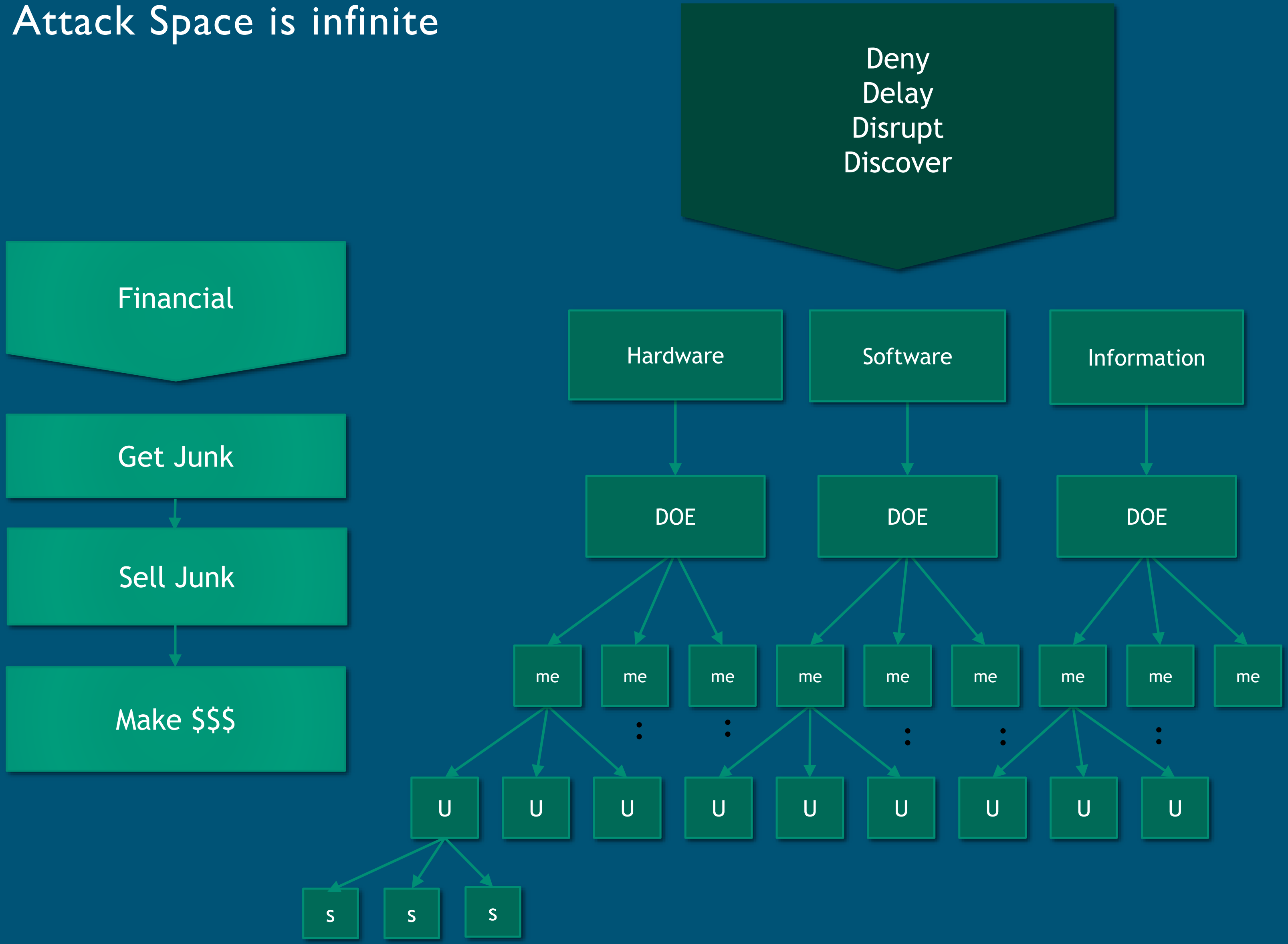
- ❑SCRM is where we are headed
- ❑Counterfeiting
- ❑Software
- ❑Cyber Espionage
- ❑Maturing your SCRM Program

Globalization

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

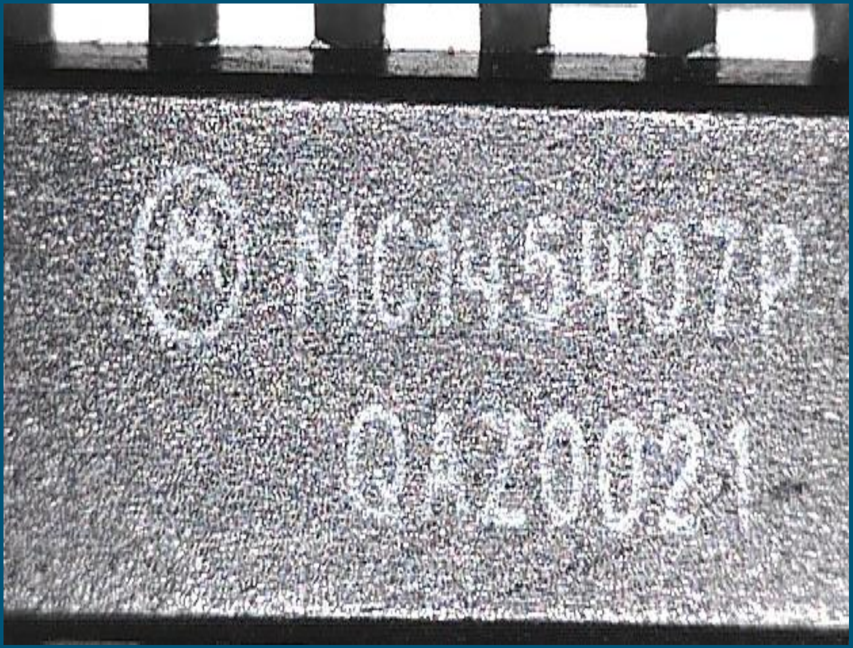
s

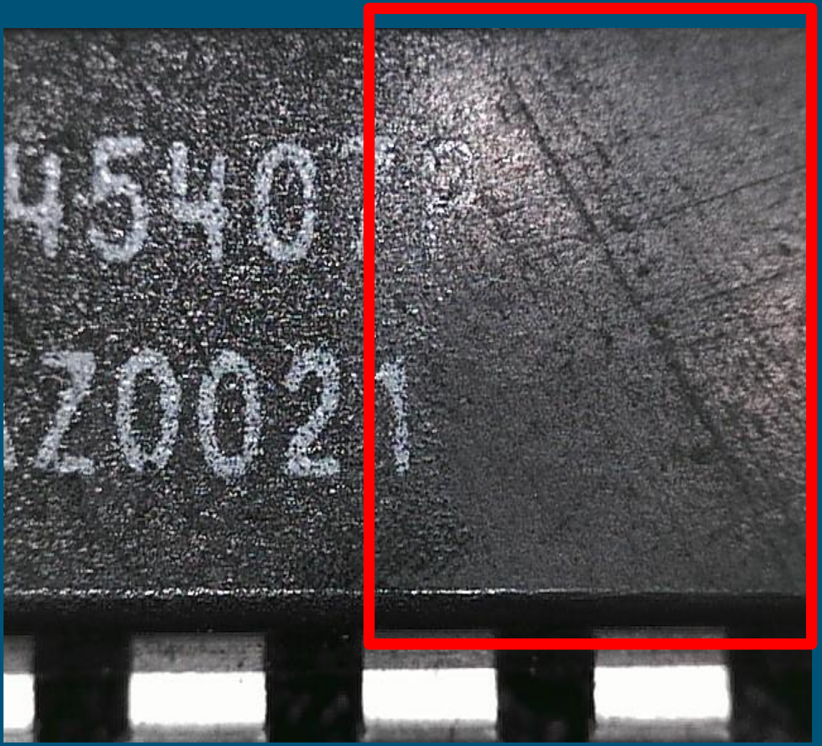
s

s

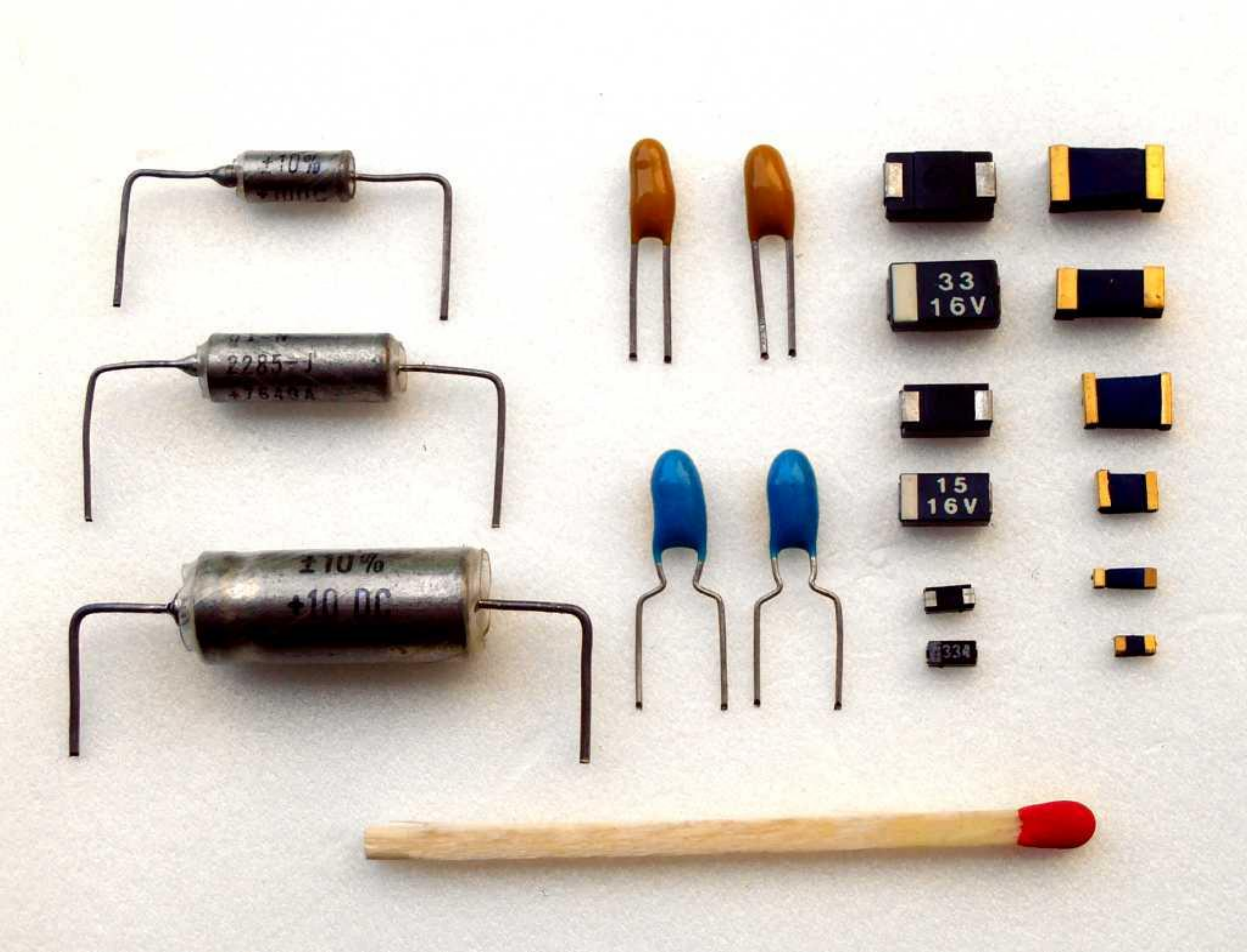
Electronics counterfeiting

Source: ERAI, Inc INSIGHT Newsletter, Q4-2018

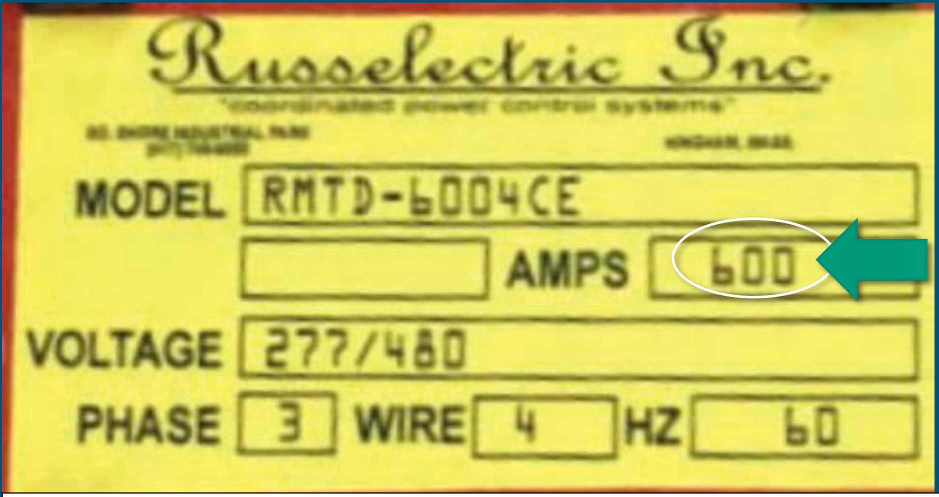




Capacitors



Electronics counterfeiting



Russelectric Inc.

"coordinated power control systems"

SO. SHORE INDUSTRIAL PARK
[illegible]

HINGHAM, MASS.

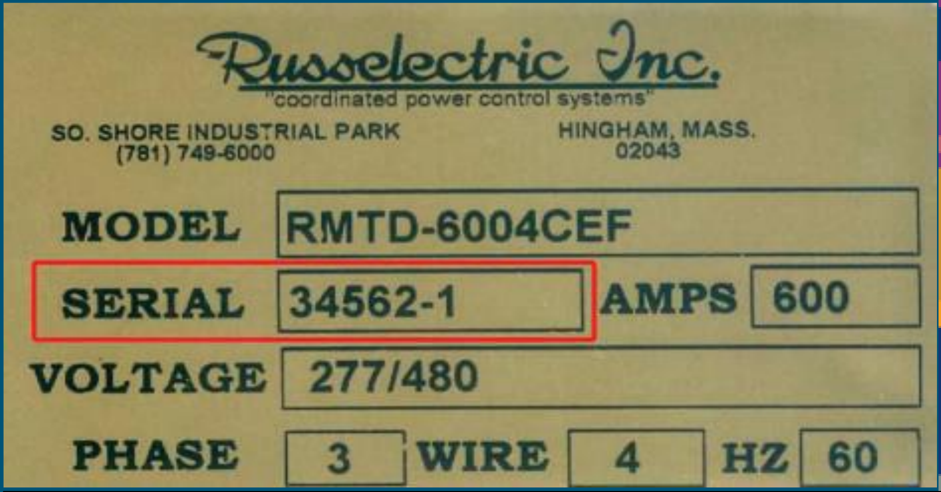
MODEL RMTD-6004CE

AMPS 600

VOLTAGE 277/480

PHASE 3 WIRE 4 HZ 60

Counterfeit label



Russelectric Inc.

"coordinated power control systems"

SO. SHORE INDUSTRIAL PARK
(781) 749-6000

HINGHAM, MASS.
02043

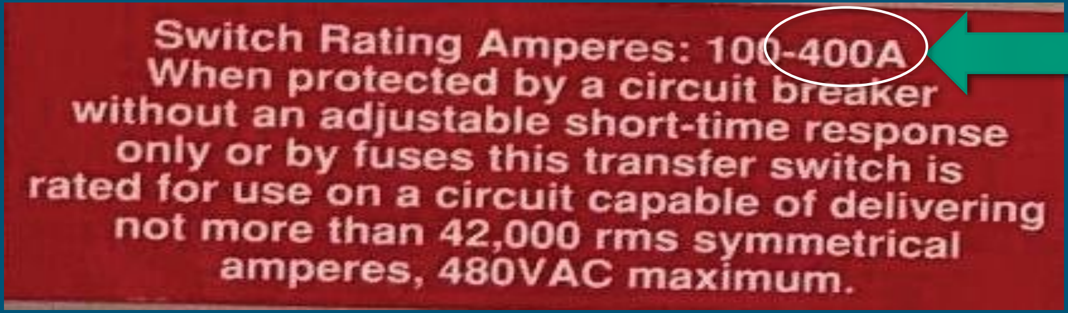
MODEL RMTD-6004CEF

SERIAL 34562-1 AMPS 600

VOLTAGE 277/480

PHASE 3 WIRE 4 HZ 60

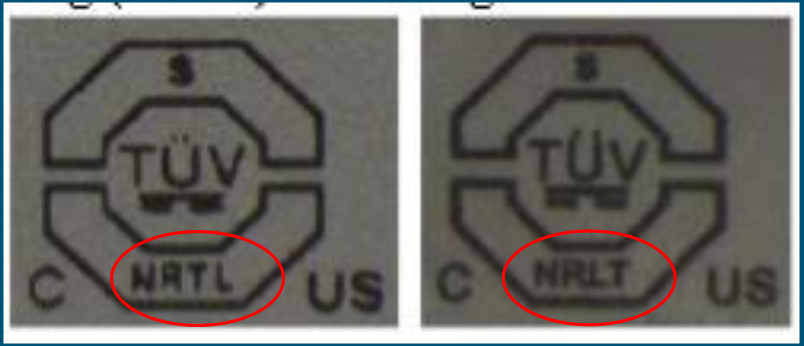
Real label example from Russelectric, Inc.



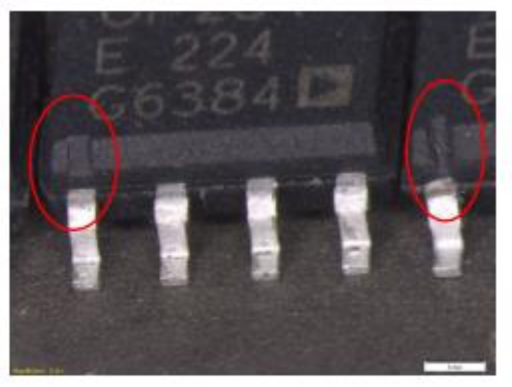
Switch Rating Amperes: 100-400A
When protected by a circuit breaker
without an adjustable short-time response
only or by fuses this transfer switch is
rated for use on a circuit capable of delivering
not more than 42,000 rms symmetrical
amperes, 480VAC maximum.

EVEN YOU can inspect deliverables!

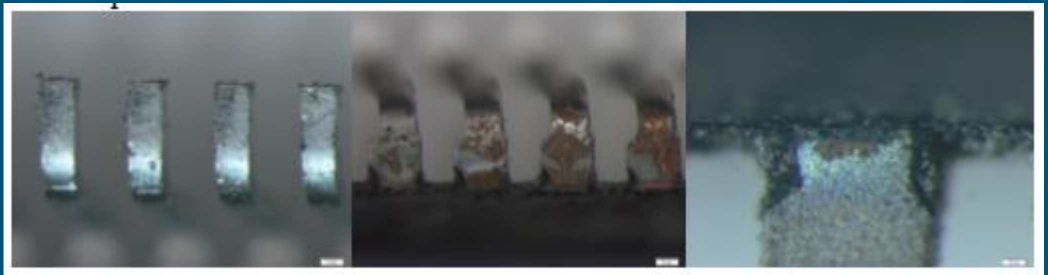
Nationally Recognized Test Laboratories



Different Pin Indicators in same lot?

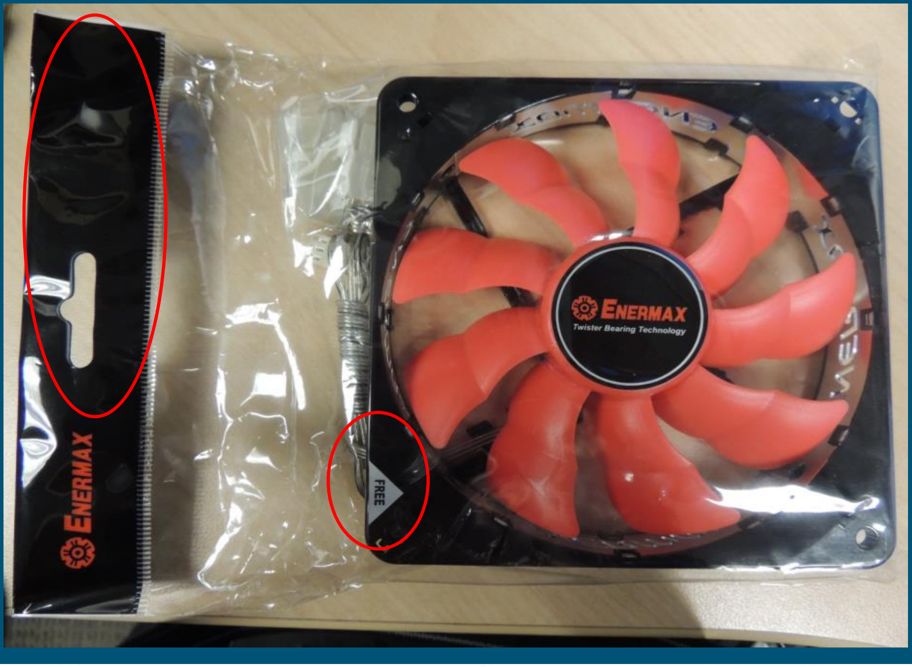


Contamination and scratches on leads?

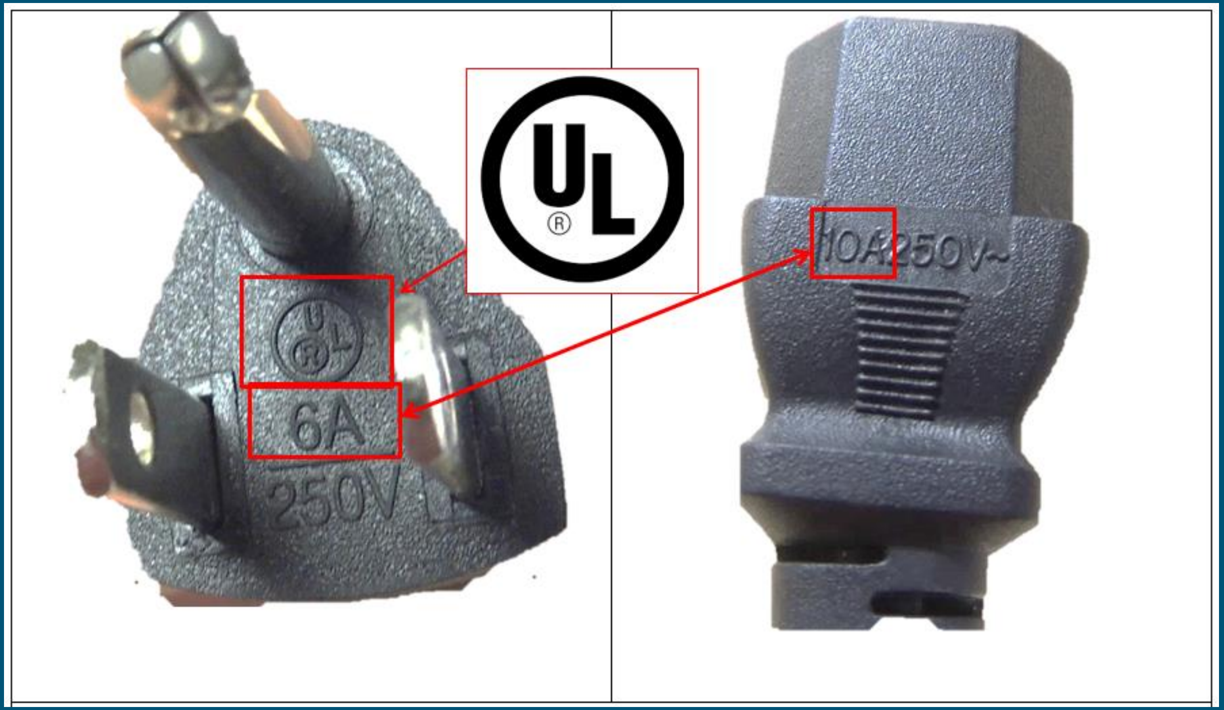


Inspection Samples

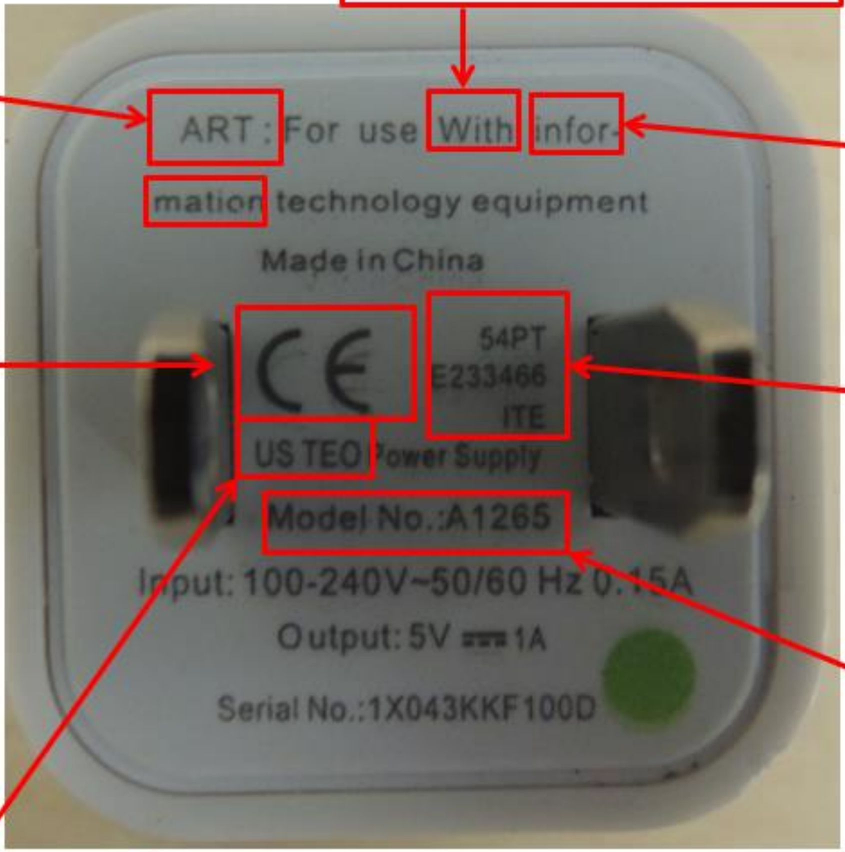
- Lack of markings on product bag
- In lower corner of fan it states “Free”



- Conflicting information: 6A on one side and 10A on the other side.
- Incorrect UL Logo format



CASE2015011- Phone Charger
TRAINING SHEET
ISSUE DATE: 03/23/2016



“With” is capitalized when normally it is not

“ART” is not a genuine company

Infor-mation is split instead of one continuous word

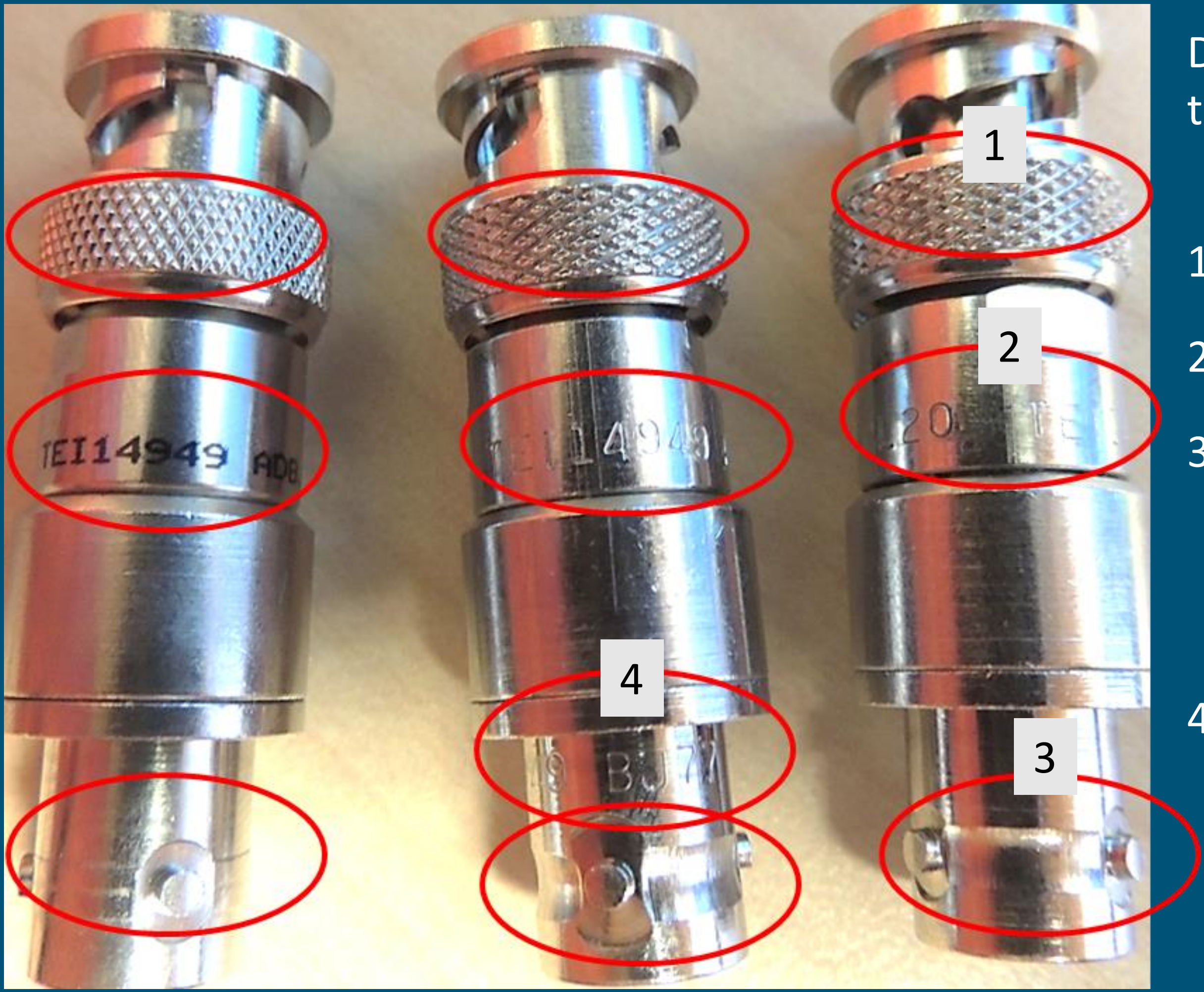
“CE” symbol looks to have been stamped over (CE is also not recognized as an NRTL mark in the US for electrical safety like UL or ETL)

“E233466”is a UL number but this is not UL certified

Model# A1265 is associated with Apple phone chargers

“US TEO” should actually read “LISTED”

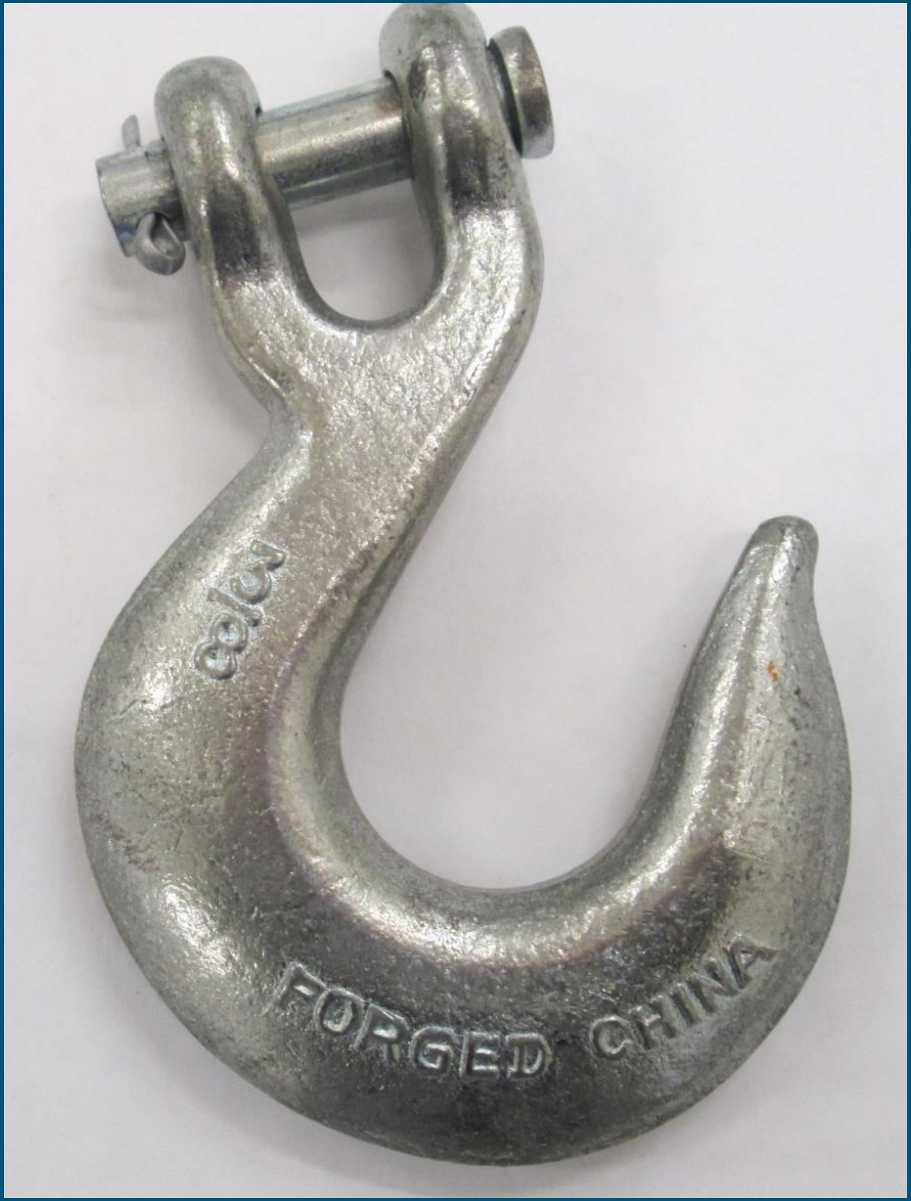
Inspection Samples



Differences between the three connectors:

1. Knurl nut is different
2. Part# print is different
3. There is a distinct groove required on the drawing that is missing on 1 pc
4. 1 pc has extra print below bushing

Quality inspections for ES&H reasons

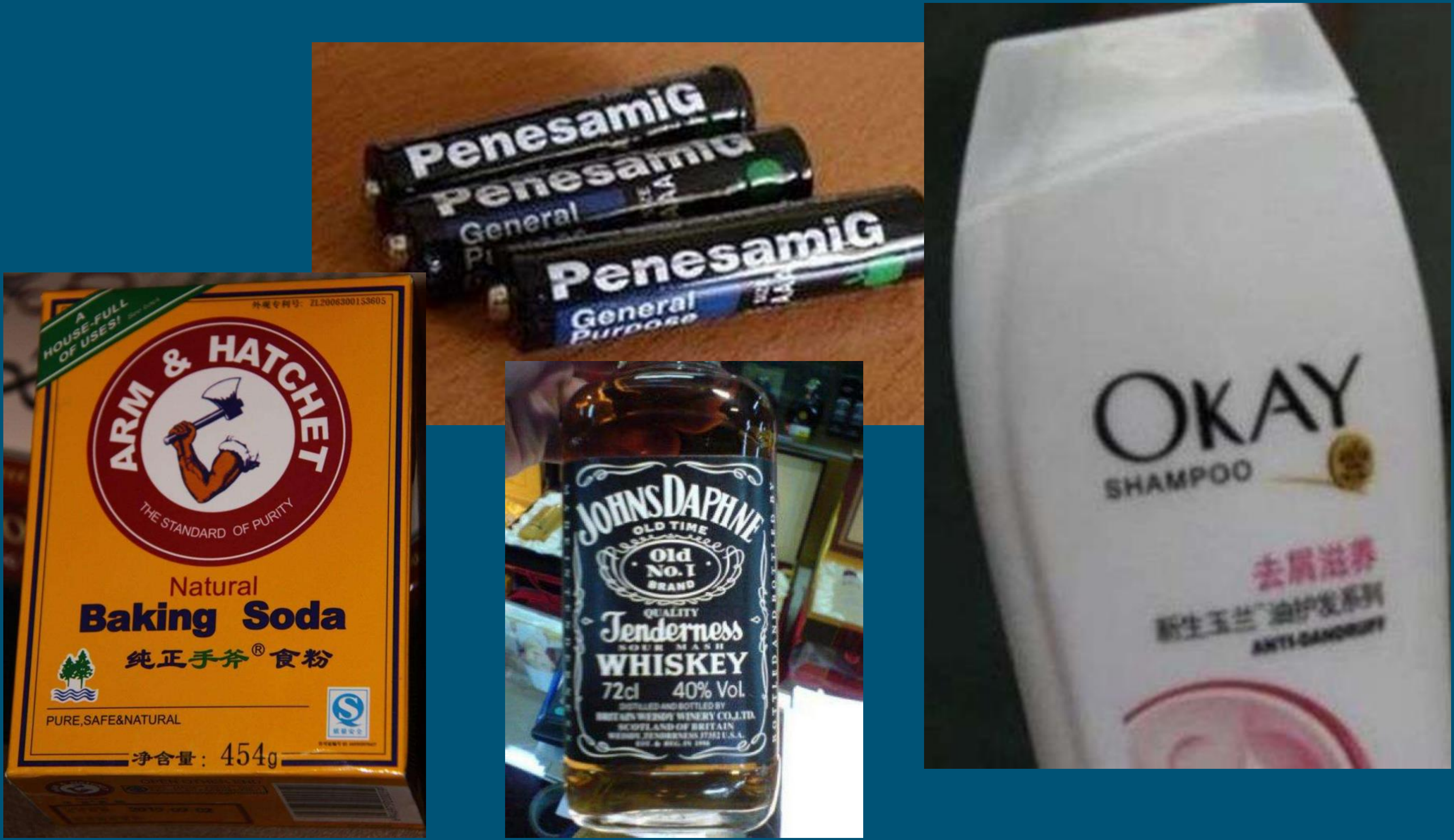


Hook is missing key features required such as:

1. Working Load Limit (WLL)

2. Manufacturer Marking or Insignia

Things you might find and want to avoid!



Top Ten General Inspection Indicators

1. Packaging (unusual or inadequate)
2. Markings, Labels, & Logos (missing, misspelled, incorrect info.)
3. General Appearance (looks used when ordered new)
4. Evidence of tampering
5. Conflicting information
6. Item is expired when received or expiration date looks to have been altered
7. Use of improper English and misspellings in instructions, warnings, or warranties provided with item
8. Item looks different than others.
9. Type of part is no longer manufactured, product is expired, has been previously recalled, or design has changed.
10. Items do not fit well or do not work properly

Other Resources

Government Aid with Intellectual Property Rights Information & Assistance: www.stopfakes.gov

US Patent and Trademark Office: www.uspto.gov

US Consumer Product Safety Commission: www.cpsc.gov

Federal Trade Commission: www.ftc.gov

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

International Trademark Association: www.inta.org

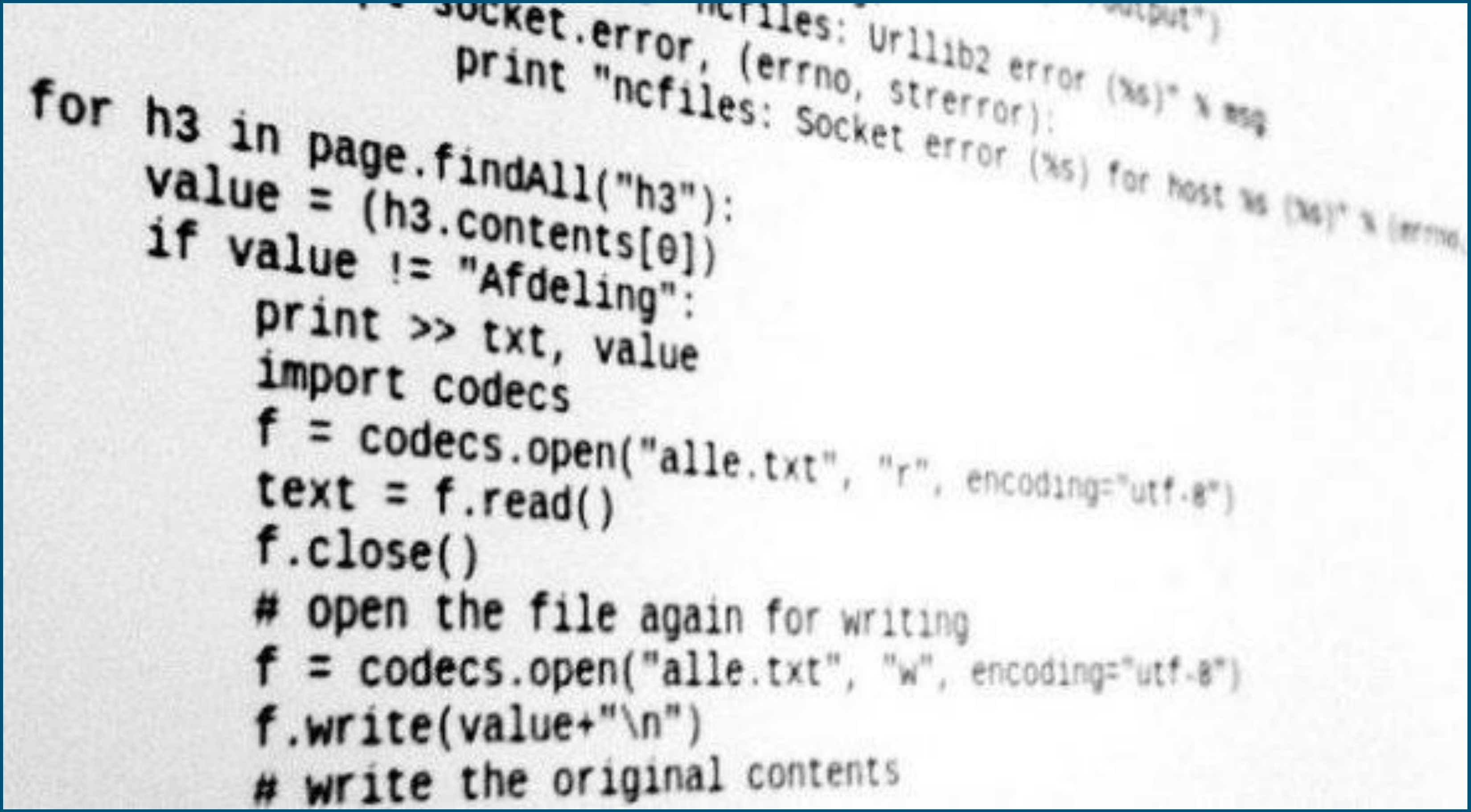
Government Industry Data Exchange Program (GIDEP): www.gidep.org

https://www.aeri.com/counterfeit-electronic-component-detection/

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



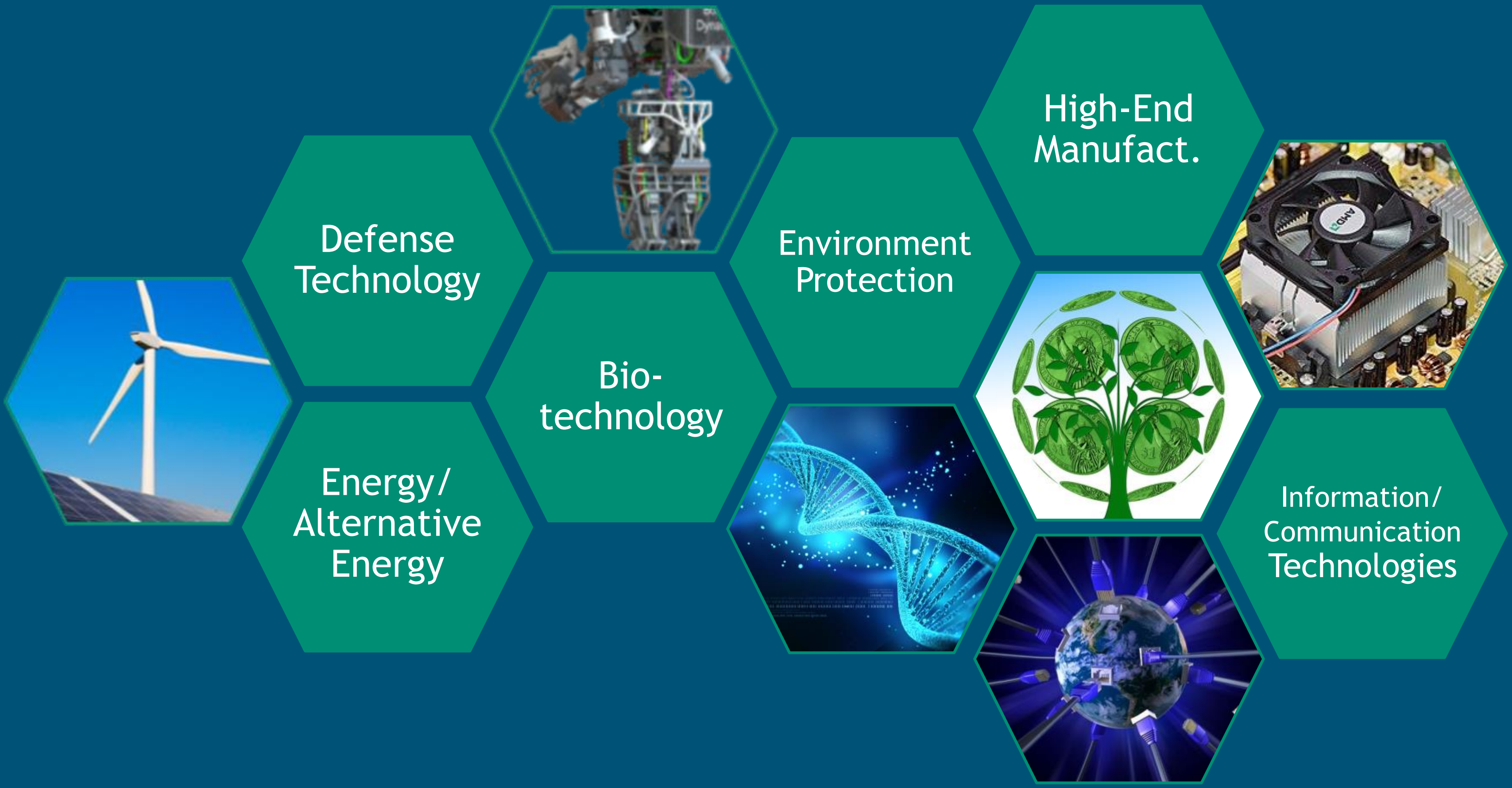
```
                                               output")
                        ncfiles: Urllib2 error (%s)" % msg
             socket.error, (errno, strerror):
                print "ncfiles: Socket error (%s) for host %s (%s)" % (errno,
for h3 in page.findAll("h3"):
    value = (h3.contents[0])
    if value != "Afdeling":
        print >> txt, value
        import codecs
        f = codecs.open("alle.txt", "r", encoding="utf-8")
        text = f.read()
        f.close()
        # open the file again for writing
        f = codecs.open("alle.txt", "w", encoding="utf-8")
        f.write(value+"\n")
        # write the original contents
```

Source: “Foreign Economic Espionage in Cyberspace”, National Counterintelligence and Security Center, 2018, https://www.dni.gov/index.php/ncsc-home

Even YOU can practice SCRM for software

1. Use and update your antivirus software.
2. Before you download or purchase software:
   - https://nvd.nist.gov/vuln/search: National Vulnerability Database. Use broad search criteria
   - http://cve.mitre.org/cve/search_cve_list.html: Common Vulnerabilities and Exposures. Use broad search criteria.
   - Read the documentation to fully understand all the functions and features (ex. wireless features)
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?

Cyber Espionage: Industries of Interest



Defense Technology

Energy/ Alternative Energy

Bio-technology

Environment Protection

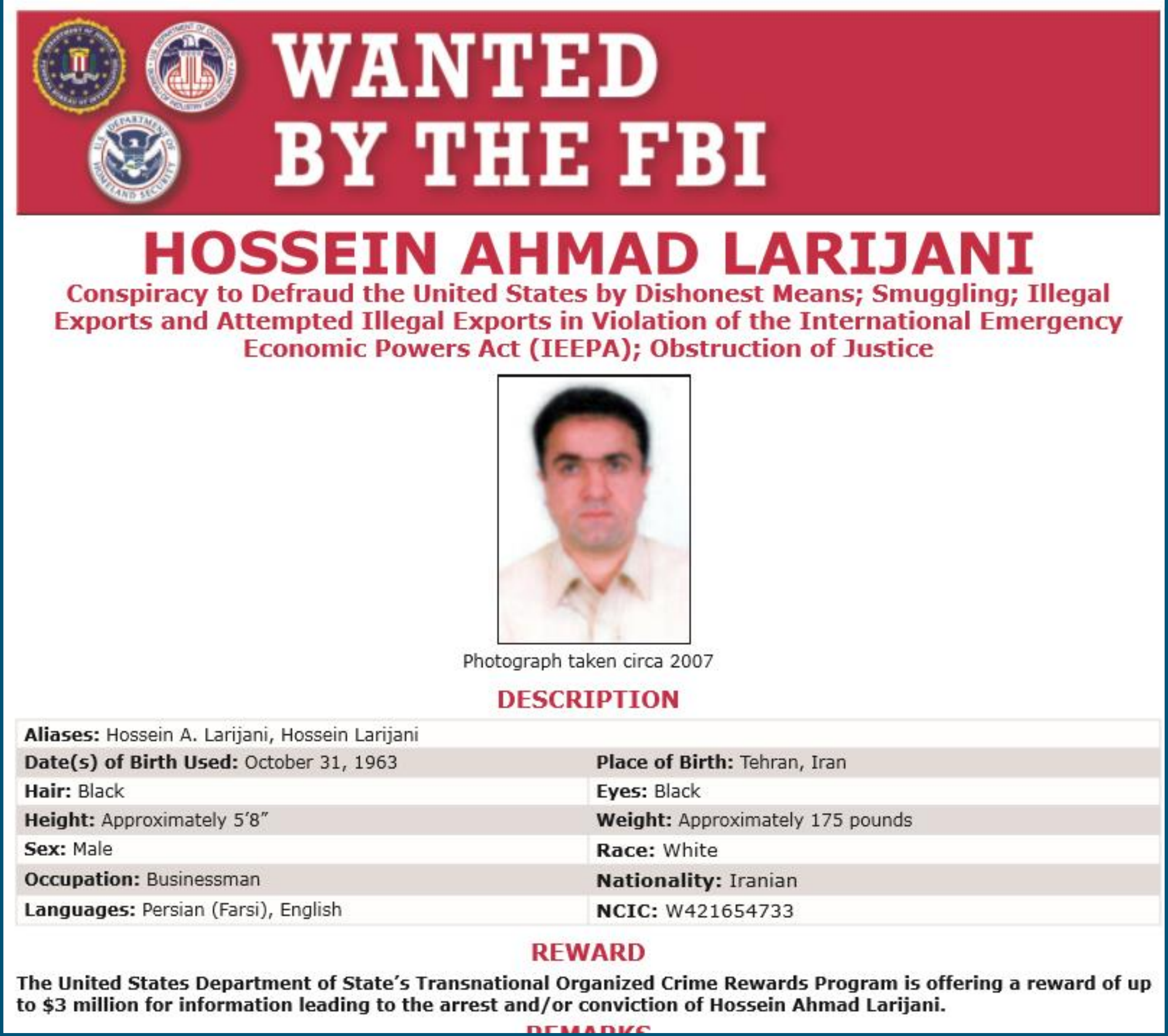
High-End Manufact.

Information/ Communication Technologies

Source: “Foreign Economic Espionage in Cyberspace”, National Counterintelligence and Security Center, 2018, https://www.dni.gov/index.php/ncsc-home

Iran

Source: “Foreign Economic Espionage in Cyberspace”, National Counterintelligence and Security Center, 2018, https://www.dni.gov/index.php/ncsc-home



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

Aliases: Hossein A. Larijani, Hossein Larijani	
Date(s) of Birth Used: October 31, 1963	**Place of Birth:** Tehran, Iran
Hair: Black	**Eyes:** Black
Height: Approximately 5'8"	**Weight:** Approximately 175 pounds
Sex: Male	**Race:** White
Occupation: Businessman	**Nationality:** Iranian
Languages: Persian (Farsi), English	**NCIC:** W421654733

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

China

Source: “Foreign Economic Espionage in Cyberspace”, National Counterintelligence and Security Center, 2018, https://www.dni.gov/index.php/ncsc-home

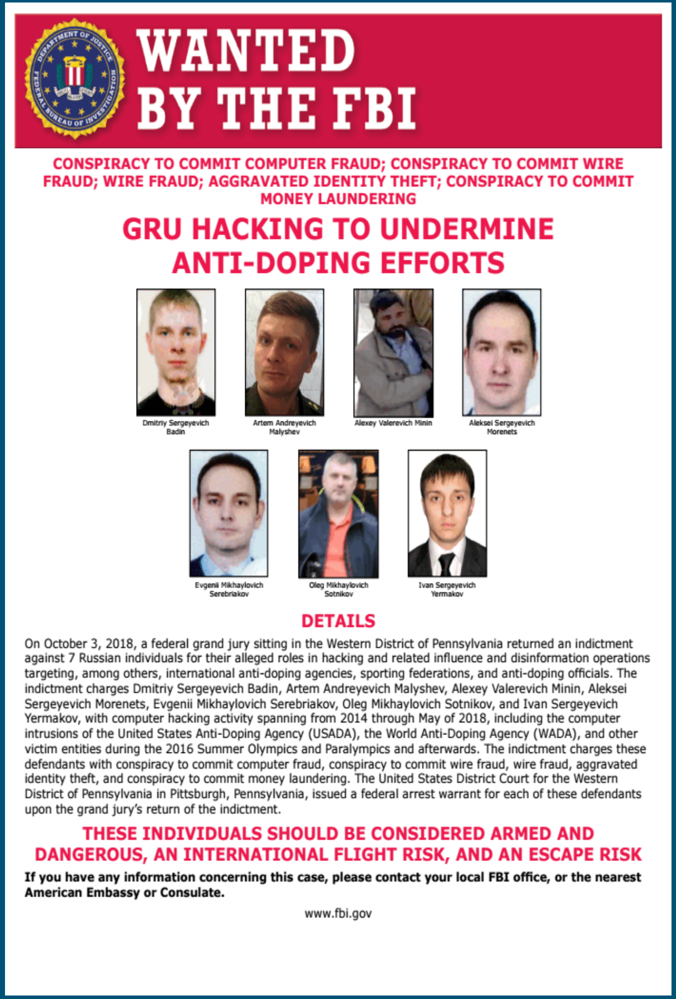
Information: Sanctions and Export Violations

Sources: ERAI, Inc INSIGHT Newsletter, Q4-2018; www.straitstimes.com; www.justice.gov

Russia

Source: “Foreign Economic Espionage in Cyberspace”, National Counterintelligence and Security Center, 2018, https://www.dni.gov/index.php/ncsc-home

Russia



WANTED BY THE FBI

CONSPIRACY TO COMMIT COMPUTER FRAUD; CONSPIRACY TO COMMIT WIRE FRAUD; WIRE FRAUD; AGGRAVATED IDENTITY THEFT; CONSPIRACY TO COMMIT MONEY LAUNDERING

GRU HACKING TO UNDERMINE ANTI-DOPING EFFORTS

Dmitriy Sergeyevich Badin

Artem Andreyevich Malyshev

Alexey Valerevich Minin

Aleksei Sergeyevich Morenets

Evgenii Mikhaylovich Serebriakov

Oleg Mikhaylovich Sotnikov

Ivan Sergeyevich Yermakov

DETAILS

On October 3, 2018, a federal grand jury sitting in the Western District of Pennsylvania returned an indictment against 7 Russian individuals for their alleged roles in hacking and related influence and disinformation operations targeting, among others, international anti-doping agencies, sporting federations, and anti-doping officials. The indictment charges Dmitriy Sergeyevich Badin, Artem Andreyevich Malyshev, Alexey Valerevich Minin, Aleksei Sergeyevich Morenets, Evgenii Mikhaylovich Serebriakov, Oleg Mikhaylovich Sotnikov, and Ivan Sergeyevich Yermakov, with computer hacking activity spanning from 2014 through May of 2018, including the computer intrusions of the United States Anti-Doping Agency (USADA), the World Anti-Doping Agency (WADA), and other victim entities during the 2016 Summer Olympics and Paralympics and afterwards. The indictment charges these defendants with conspiracy to commit computer fraud, conspiracy to commit wire fraud, wire fraud, aggravated identity theft, and conspiracy to commit money laundering. The United States District Court for the Western District of Pennsylvania in Pittsburgh, Pennsylvania, issued a federal arrest warrant for each of these defendants upon the grand jury's return of the indictment.

THESE INDIVIDUALS SHOULD BE CONSIDERED ARMED AND DANGEROUS, AN INTERNATIONAL FLIGHT RISK, AND AN ESCAPE RISK

If you have any information concerning this case, please contact your local FBI office, or the nearest American Embassy or Consulate.

www.fbi.gov

Source: https://www.fbi.gov/news/stories/russian-gru-officers-charged-with-hacking-100418

Even YOU can Practice Basic Cybersecurity!

Understanding the NIST Cybersecurity Framework

Physical Security

Ransomware

Cybersecurity Basics

Phishing

Federal Trade Commission: https://www.ftc.gov/SmallBusiness

Securing Remote Access

Business Email Imposters

Hiring a Web Host

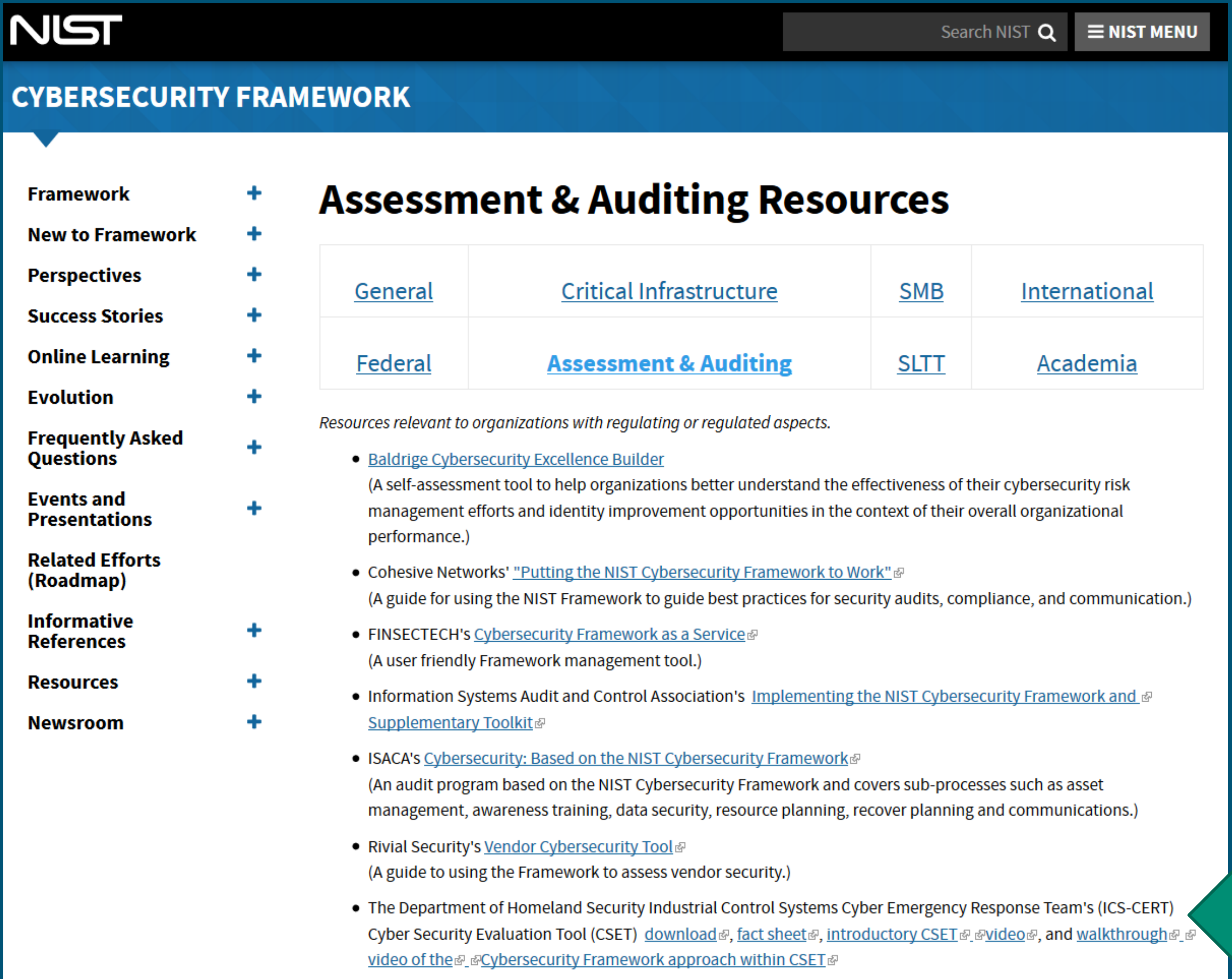
Tech Support Scams

Email Authentication

Cyber Insurance

Vendor Security

Even YOU can Practice Basic Cybersecurity!



Assessment & Auditing Resources

General	Critical Infrastructure	SMB	International
Federal	**Assessment & Auditing**	SLTT	Academia

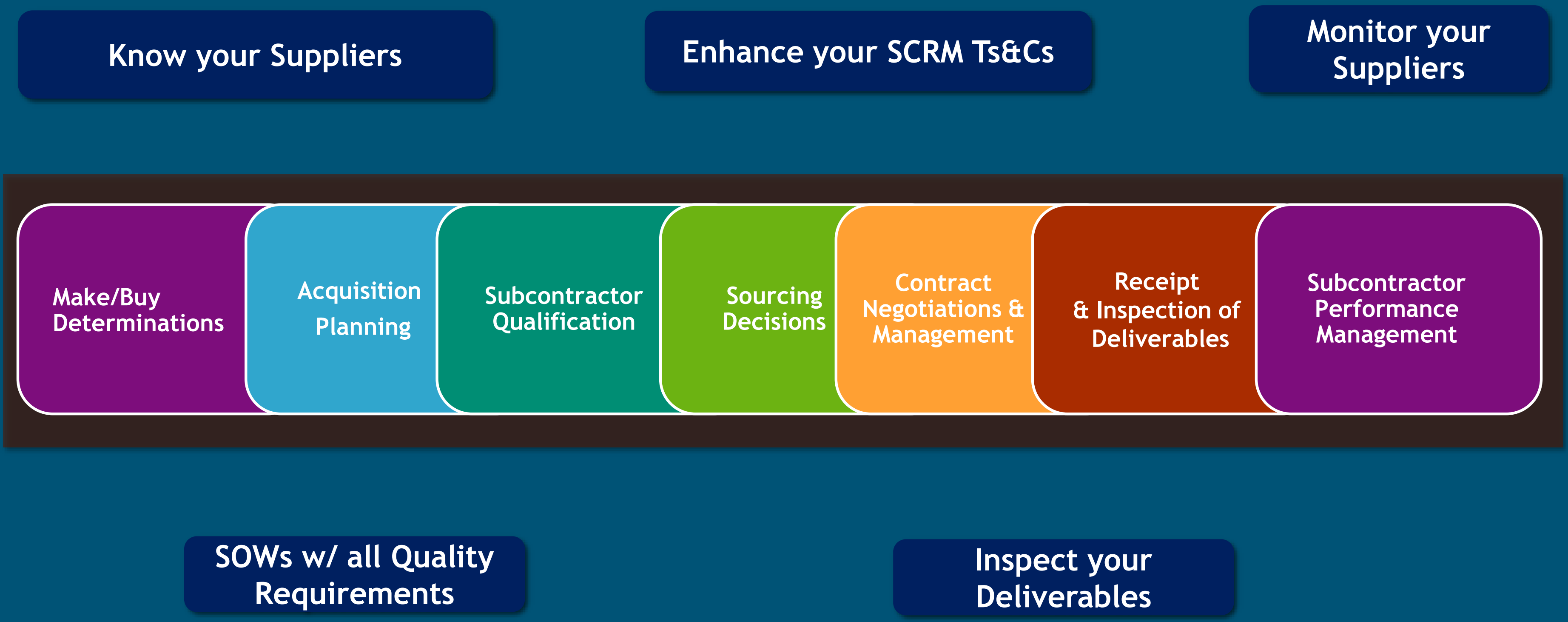
Resources relevant to organizations with regulating or regulated aspects.

- Baldrige Cybersecurity Excellence Builder
(A self-assessment tool to help organizations better understand the effectiveness of their cybersecurity risk management efforts and identity 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.)
- FINSECTECH'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.)
- The Department of Homeland Security Industrial Control Systems Cyber Emergency Response Team's (ICS-CERT) Cyber Security Evaluation Tool (CSET) download, fact sheet, introductory CSET video, and walkthrough video of the Cybersecurity Framework approach within CSET

CSET TOOL

https://www.nist.gov/cyberframework/assessment-auditing-resources

Maturing your SCRM practices



Know your Suppliers

Enhance your SCRM Ts&Cs

Monitor your Suppliers

Make/Buy Determinations

Acquisition Planning

Subcontractor Qualification

Sourcing Decisions

Contract Negotiations & Management

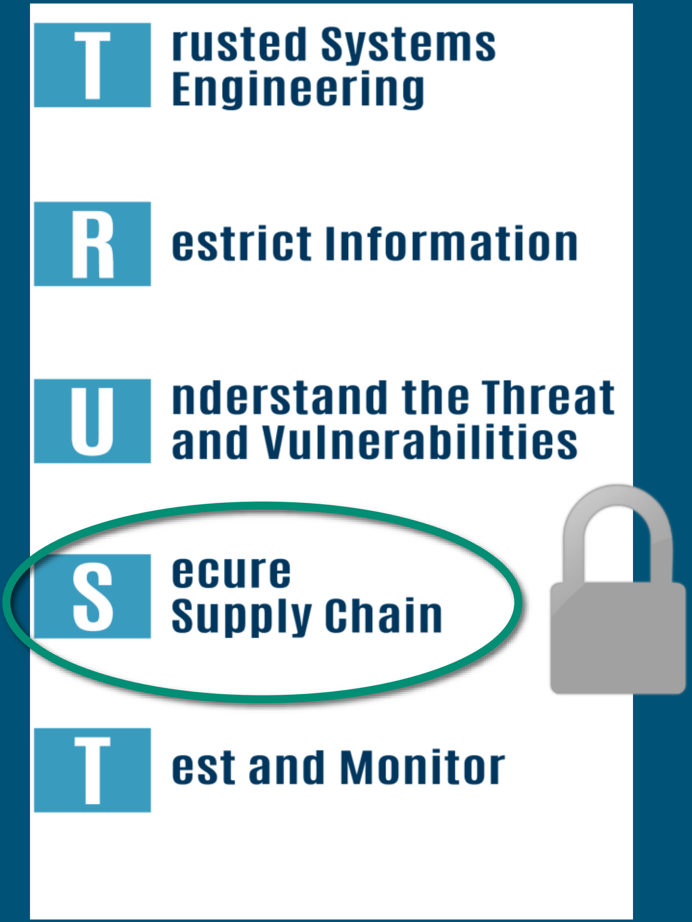
Receipt & Inspection of Deliverables

Subcontractor Performance Management

SOWs w/ all Quality Requirements

Inspect your Deliverables

Relevant Policies and Potential Flowdowns



T rusted Systems Engineering

R estrict Information

U nderstand the Threat and Vulnerabilities

S ecure Supply Chain

T est and Monitor

- 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!

Technical information

Potential and approved designs

Production materials, components, technologies, and problems (including solutions)

Science and technology innovations

Project management information

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

Connections/Contacts

Employment/ partnership/ conference interaction opportunities

Leadership/personnel identification

Potential and selected vendors/contractors

Successes/awards

Caution in Advertising

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

Session Evaluations

Reminder

Please complete the Speaker/Session Evaluation Form located in the Mobile App.

Response to question during session about resources/information relating to social media

Helpful information regarding security settings for social media:

https://www.dla.mil/Portals/104/Users/230/98/998/DoD_Identity_Awarness_Protection_Management_Guide_September_2018.pdf?ver=2018-12-21-082234-527