Supply Chain Surety Industry Workshop

25 May 2017

Time	Event	Presenter/Facilitator
0840-0845	Welcome	NDIA
0845-0900	OPNAV Introduction	VADM Dixon Smith
0900-0910	Joint Staff Brief	VADM William Brown
0910-1000	DOD and US Government SCRM Efforts	Mr. Don Davidson
1000-1030	Review Overarching Theme and Questions	RDML John Polowczyk
1030-1040	OSD L&MR	Ms. Kristin French
1040-1100	Break	NDIA
1100-1115	Breakout Session Instructions	Groups
1115-1215	Strategic Breakout Group	Flag/SES
1115-1215	Breakout Sessions	Groups
1215-1300	Lunch	
1300-1430	Breakout Sessions Resume	Groups
1430-1500	Break / Group Leaders Prepare Summary	Groups
1500-1600	Brief Recommendations / Summarize / Adjourn	Group Leads

Joint Staff J4 Perspective

Supply Chain Surety Workshop

VADM William A. Brown
The Joint Staff, Directorate of Logistics, J4

Defense Industrial Base Framework

***Problem* Statement:**

Analyze the nation's ability to surge the industrial base to determine if additional authorities, programs, policies and partnerships are needed to shorten the Defense Industrial Base's response time to support the military supply chain during a large scale conflict.

Defense Industrial Base Framework

Sectors:

Energy / Engineering

Munitions / Missiles

Mobility / Transportation

Strategic Materials

Electronics / Cyber

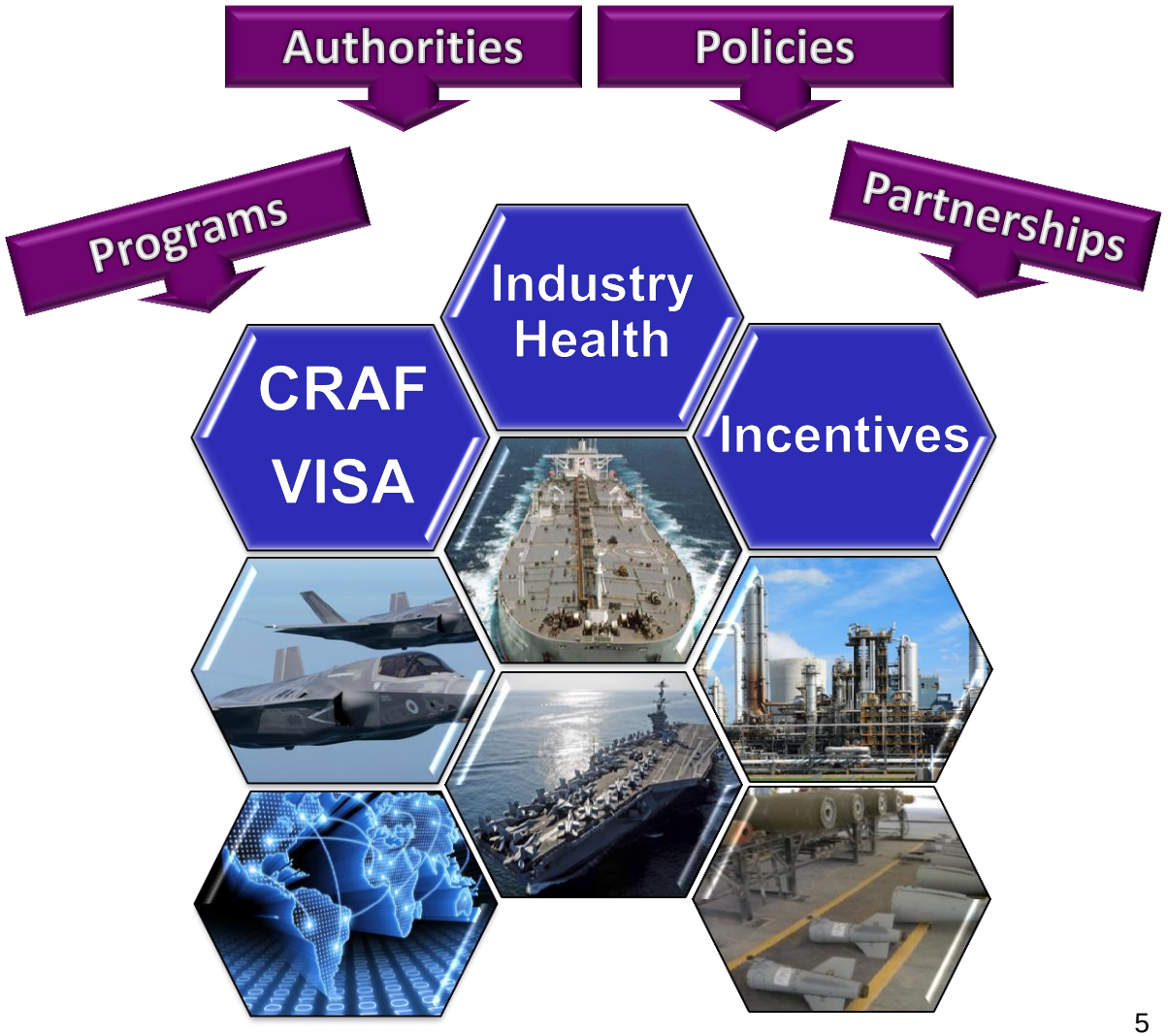
Aircraft

Ships

Ground Vehicles / Equipment

Space

Emerging Sectors



Supply Chain Risk Management
Current Environment

RDML John Polowczyk

OPNAV N41

Navigating The Current Environment

Surety

Enablers

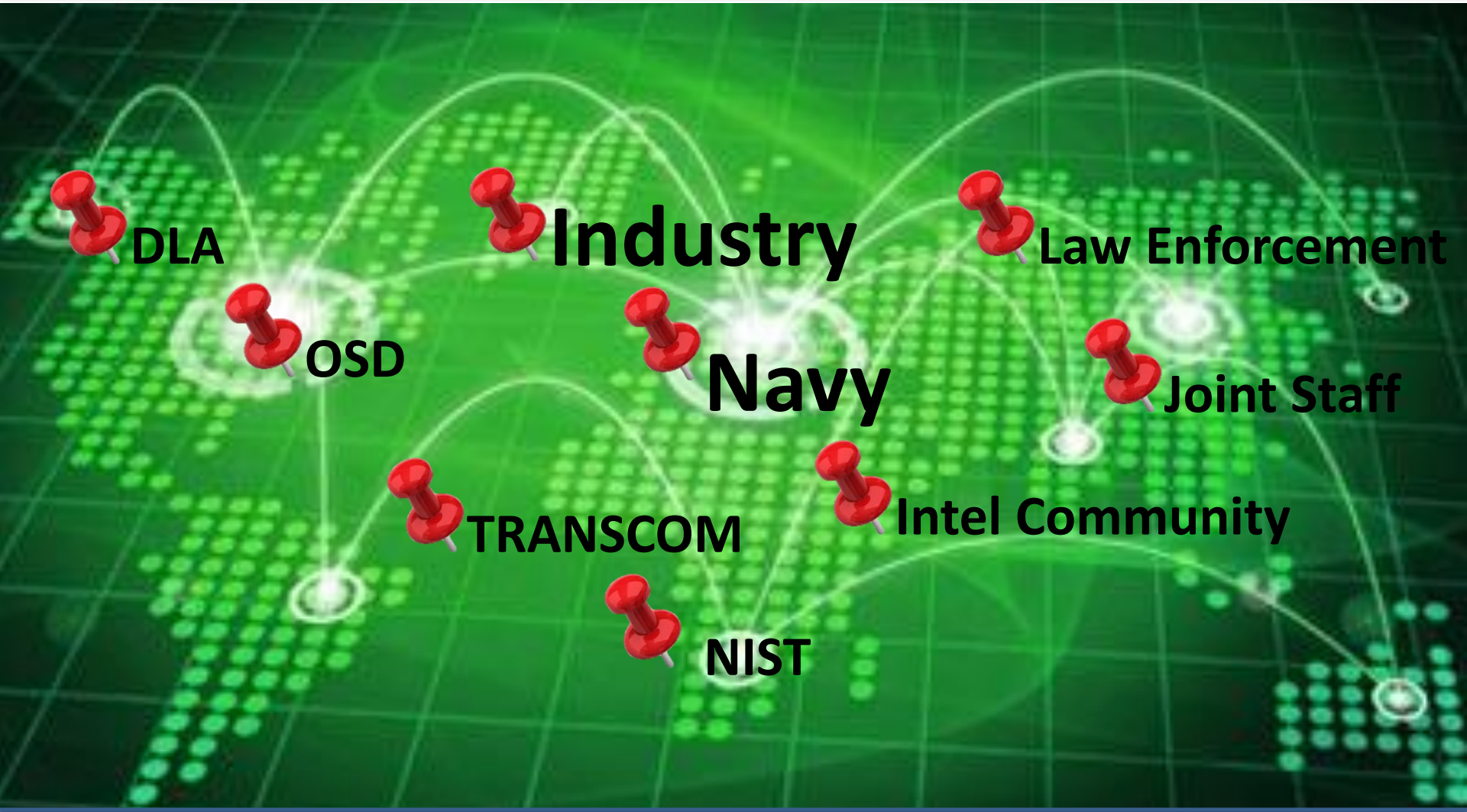
- Rise Of Big Data
- Globalization
- Technology Proliferation

Risks

- Easier Access To Data
- Foreign Competition
- Lower barrier to entry

Embrace And Leverage Enablers → Mitigate Risk

Collaboration Is Key



Surety is a “Team Sport”

Disparate Efforts Across DoD

Policies & Procedures


The White House
Office of the Press Secretary
For Immediate Release — May 11, 2017

Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure

EXECUTIVE ORDER

STRENGTHENING THE CYBERSECURITY OF FEDERAL NETWORKS AND CRITICAL INFRASTRUCTURE

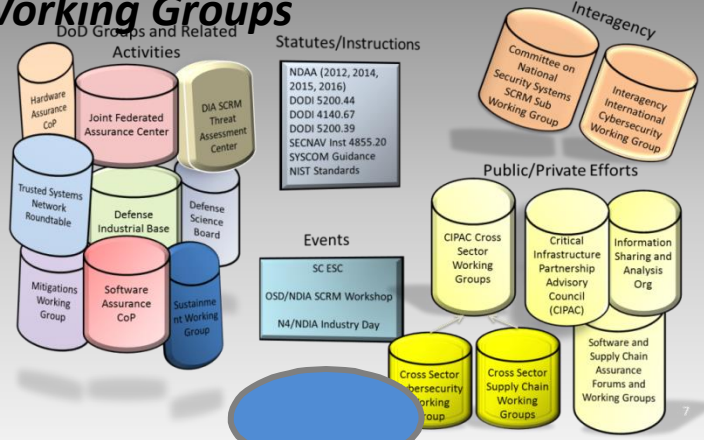
By the authority vested in me as President by the Constitution and the laws of the United States of America, and to protect American innovation and values, it is hereby ordered as follows:

Section 1. Cybersecurity of Federal Networks.

(a) Policy. The executive branch operates its information technology (IT) on behalf of the American people. Its IT and data should be secured responsibly

11 May 2017

Working Groups



- DODI 5200.44 TSN
- NDIA
- NDAA

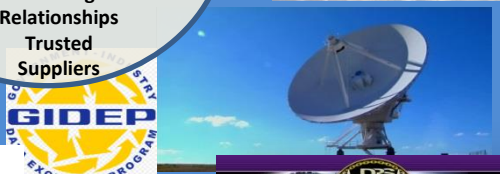
DODI 8320.04 IUID
DODI 4140.67 Counterfeit Prevention
FAR
- SECNAVINST 4855.20

- DODI 8320.04 IUID
- Joint Deficiency Reporting System
- Contract Clause/Language
- NDIA
- NDAA

Trusted Systems & Networks

Government Industry Data Exchange Program
Joint Deficiency Reporting System
Individual Unit Identification

Training
Relationships
Trusted Suppliers

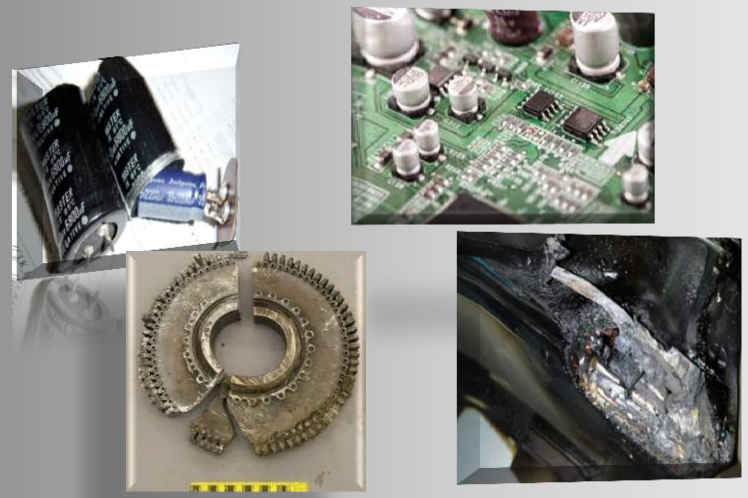


Do All the Pieces Fit?

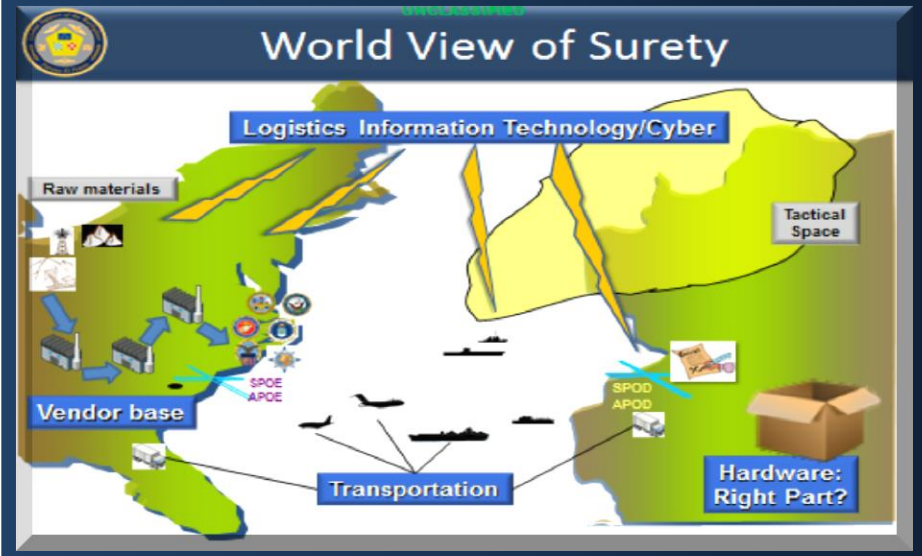
Key Challenges

IT/Cyber

Product

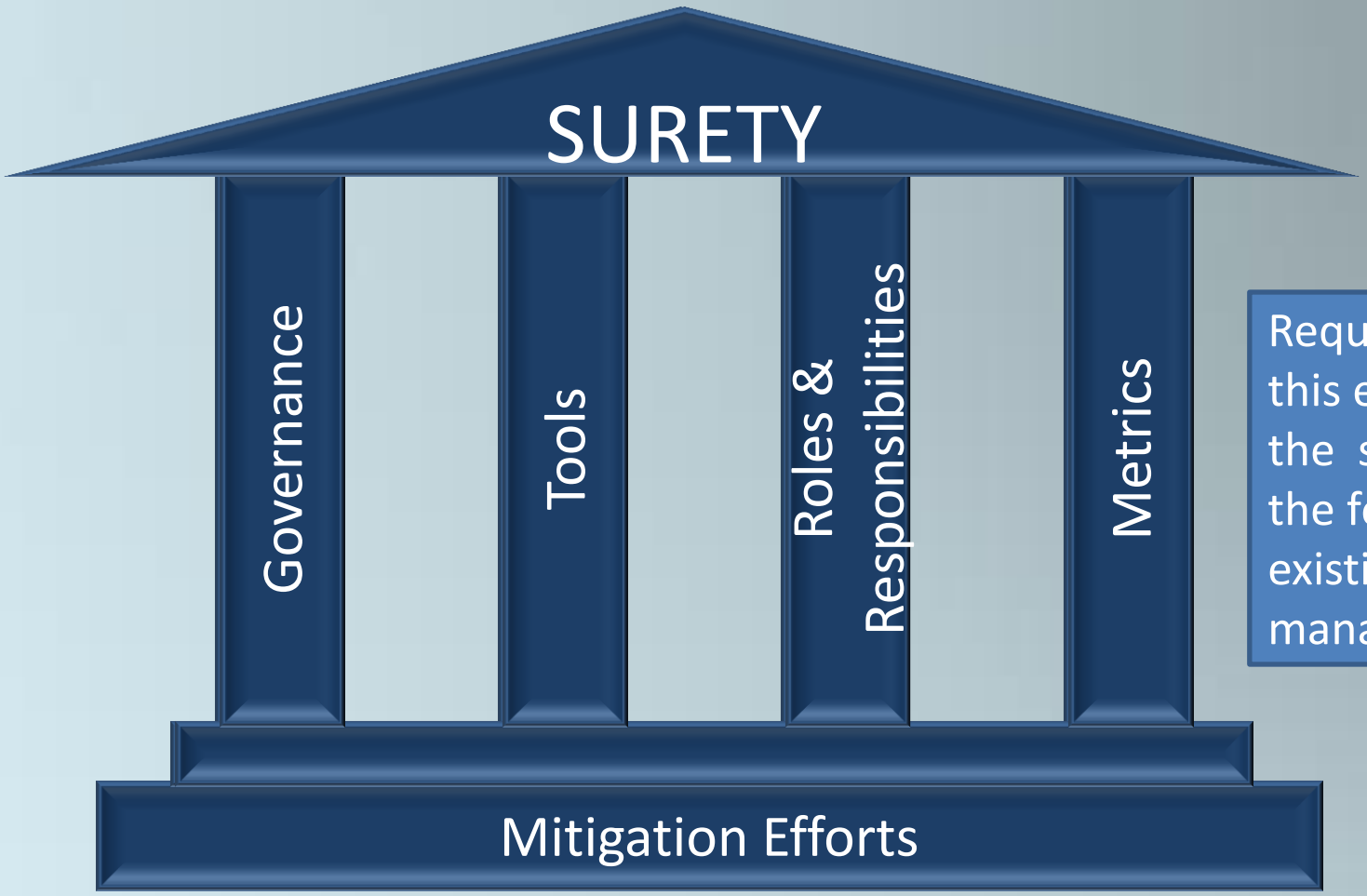


Distribution



Vendor Certification

First Waypoint



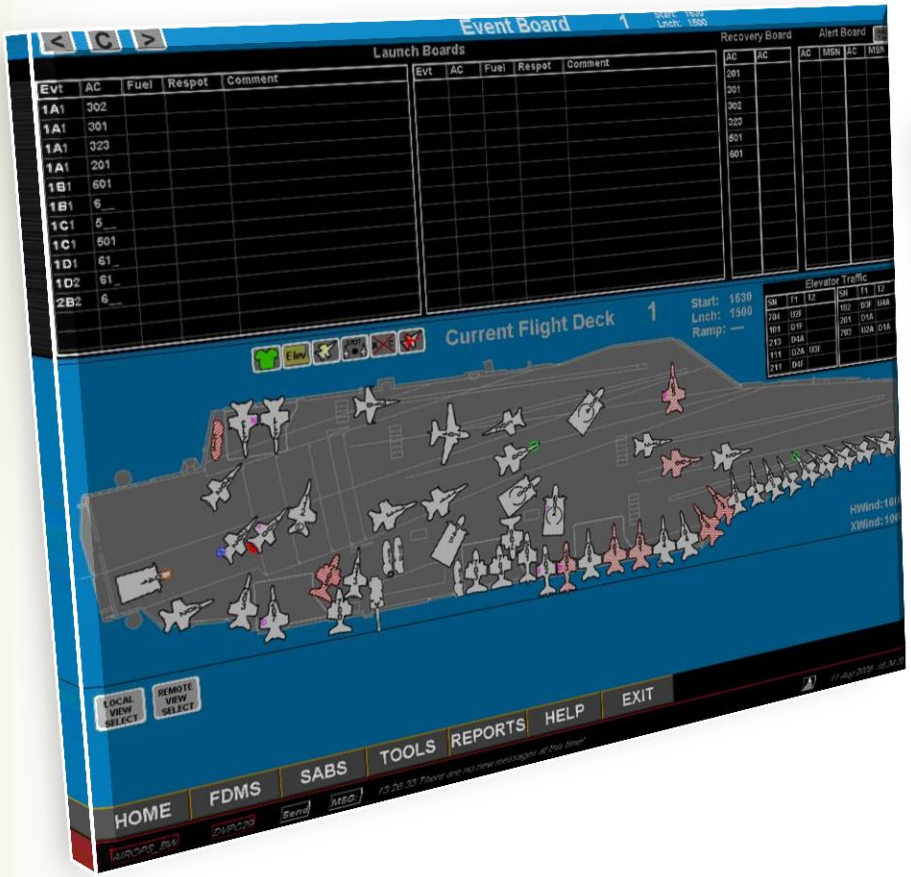
Required outcome of this effort is to build the surety pillars on the foundation of the existing risk management efforts

Building the Pillars

OSD L&MR
Ms. Kristin French

Product in Supply Chain for Surety Breakout Group

Product: ADMACS Case Study



- Aviation Data Management and Control System (ADMACS)
- Provides tactical, real-time data management system that connects the air department, ship divisions, and embarked staff who manage aircraft launch and recovery operations

ADMACS employed on CVN to manage flight deck configurations

Product: ADMACS Case Study

- Contains approximately 30 end item parts. Each of the 30 parts has multiple subcomponents with multiple potential sources of supply
- The system is assembled at a Contractor Facility (both new ships and upgrades to existing systems, then installed on ship.
- Government Software Support Activity (SSA) comes in and does loading of software/testing.
- Many of the components could be considered for standard COTS products at lower cost.
- No Product Protection Plan (PPP) Performed.

Product: Questions

- How cognizant do we have to be
- What level of trust do we place in Primes (if non-govt)?
- Paralysis by Analysis of data?
- What do we need to assess? Why?
- What is critical?
- How important is country of origin in determination?

Criticality Levels from PPP

Level I – Total Mission Failure	Function/component failure results in total compromise of mission thread
Level II – Significant/Unacceptable Degradation	Function/component failure results in unacceptable compromise of mission thread or significant mission degradation
Level III – Partial/Acceptable	Function/component failure results in partial compromise of mission thread or partial mission degradation
Level IV – Negligible	Function/component failure results in little or no compromise of mission thread

Vendor Certification in Supply Chain for Surety Breakout Group

Vendor Certification: MORIAH Case Study

- MORIAH is an advanced wind measuring system used on CVN
- OEM is a British company
- Uses some components that were bought out by a Chinese corporation in 2014.

MORIAH employed on CVN

Vendor Certification: MORIAH Case Study

- Contains approximately 90 end item parts
- How many supplier tiers should we maintain visibility of?
- Do we need to know all?
- China Huaxin Post & Telecommunication Economy Development Center ("China Huaxin") is an industrial investment company that seeks long-term commercial growth opportunities in the **Information and Communications Technologies (ICT) sector**.

Moriah Wind System

Nomenclature	Reference number	Cage	NSN	Comments	Potential for Malicious Cod	Counterfeit Parts	Sabotage
	3771AS6129-01	30003					
Wind Sensor Unit (WSU)	81164/0200.00	0SJM3	5895-01-532-5726	Proprietary QPI		x	
Wind Processor Unit (wpu) V1	81163/0200.00W01	0SJM3		Proprietary QPI	x	x	x
Wind Processor Unit (wpu) V2	81163/0200.00W02	0SJM3		Several versions	x	x	x
Wind Processor Unit (wpu) V3	81163/0200.00W03	0SJM3		to be replaced	x	x	x
Wind Processor Unit (wpu) V4	81163/0200.00W04	0SJM3		by	x	x	x
Wind Processor Unit (wpu) V6	81163/0200.00W06	0SJM3		W06	x	x	x
Sub Processor Fibre	81163/0300.00W04	0SJM3	5895-01-599-1703	Proprietary QPI	x	x	x
Modules, GUI INTC	81163/0320.00	0SJM3	NICN LLH644132		x	x	x
ASSY, PSU	81163/0310.00W01	0SJM3	6130-01-540-2515	Proprietary QPI	x	x	x
Line Interface Unit	81163/0600.00W01	0SJM3	6660-01-522-8317	Proprietary QPI	x	x	x
Capacitor, Reservoir	PEH200MO5470MB2	31433				x	x
Filter, EMI	FN2060-10/06	F9692				x	x
Power Supply, 28VDC	P5753	58910	6130-01-608-8156			x	x
UNINTERRUPTIBLE POW	201-SS-Grade A-6MO-6P	0ZAP8	6130-01-652-4874			x	x
Battery	RBC55	0ZAP8				x	
Small Network Switch	3771AS0637-1	30003			x	x	x
Switch, OS6855-U24X	OS6855-U24X	064L4	5895-01-611-4271		x	x	x
Switch Power Supply	OS6855-PSL	064L4				x	x
Transceiver	ISFP-100-MM	064L4			x	x	x
High End Display	81161/0200.00/E	0SJM3	5895-01-532-5728	Proprietary QPI		x	x
GUI KIT, WPU	81163/0102.00	0SJM3	5895-01-538-5830			x	x
GUI KIT, HED/LED	81161/0102.00	0SJM3	5995-01-541-0096			x	x
Low End Display	81162/0200.00/E	0SJM3	6320-99-391-2385		x	x	x
FIBER BLADE	OS9-GNI-U24	0ZZJ6	GFE		x	x	x
CMM BLADE	OS9700-CMM	0ZZJ6	GFE		x	x	x
CHASSIS BUNDLE, SWITCH, 9700	OS9702-CHASSIS	0ZZJ6	GFE	Alcatel- Lucent Switch bought out by Chinese			
MODULE, MANAGEMENT & FAB	OS7700-CMM	0ZZJ6	GFE			x	x
CHASSIS BUNDLE, SWITCH, 7700	OS7700-RCB-FED	0ZZJ6	GFE	Alcatel- Lucent Switch bought out by Chinese			
TRANSCEIVER, 100BASE	SFP-DUAL-MM	0ZZJ6	GFE				
TRANSCEIVER, GIG	SFP-DUAL-SM10	0ZZJ6	GFE				
POWER DISTRIBUTION UNIT (PDU), W/ 22-INCH SLIDE	PDU-2000-3	25965	GFE				
PS, 2KVA, W/ BATTERY, W/ 28-INCH SL	M120BA-1A-1-1-0	OB7R6	GFE				

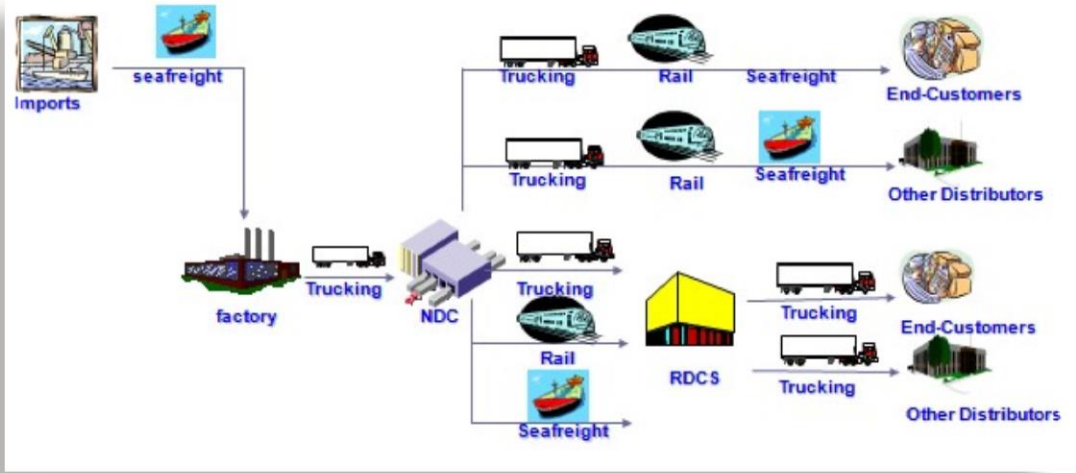
Alcatel-Lucent sells enterprise networking unit to China Huaxin in 2014

Vendor Certification: MORIAH Case Study

- Does it matter who the Lead Source Integrator (LSI) is?
- How much visibility do we need?
- What level of information do we need about suppliers?
- Do we need to know the origin of the supplier?
- Do we completely trust our allies? What if they procure parts from known bad actors?
- How do we assess what is important?

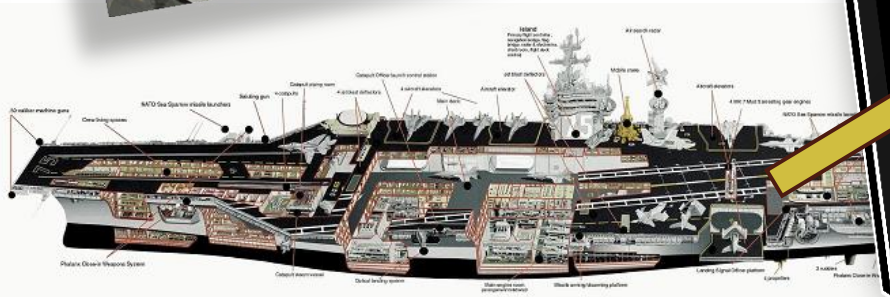
Distribution in Supply Chain for Surety Breakout Group

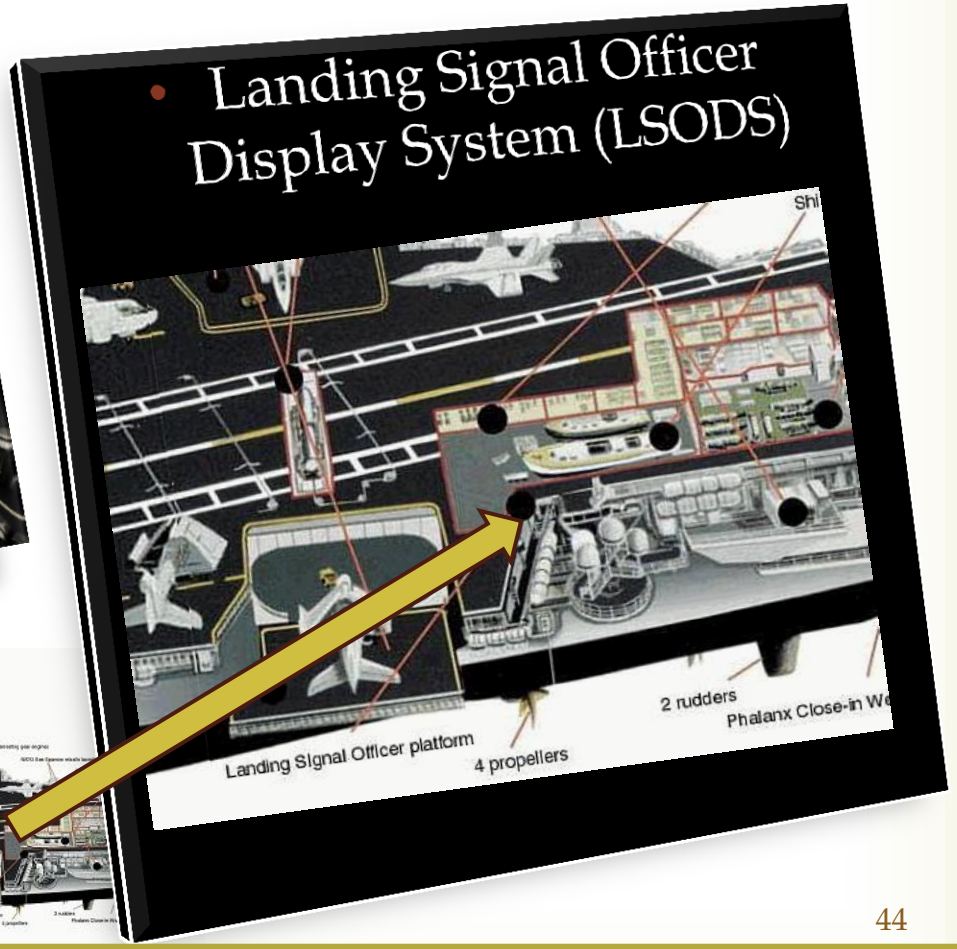
What is Distribution in the Supply Chain?



A **distribution network** is an interrelated arrangement of people, storage facilities and transportation systems that moves goods and services from producers to consumers.
A **distribution network** is the system a company uses to get products from the manufacturer to the retailer.

Distribution: LSODS Case Study

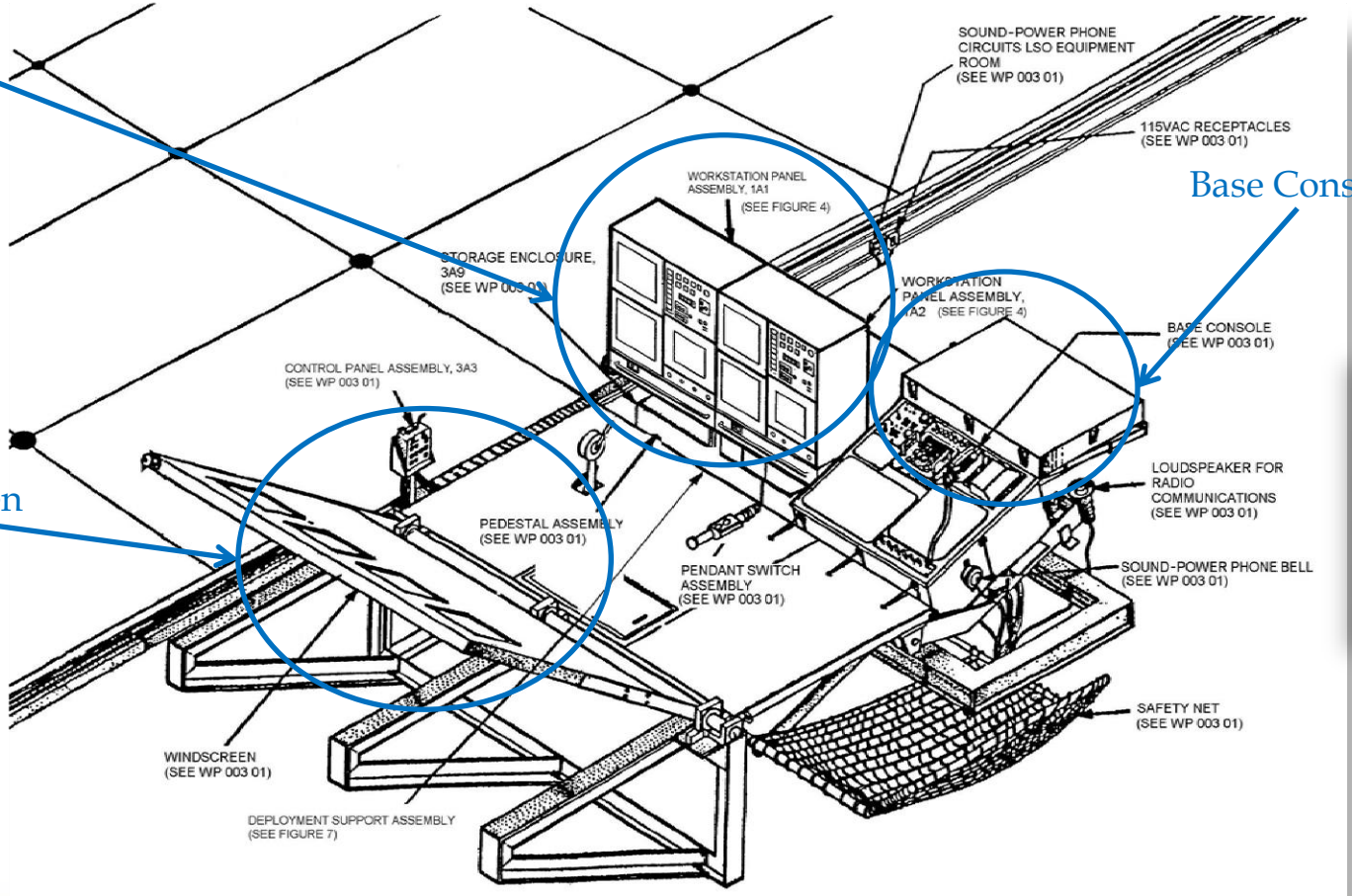




LSODS Overview
Above Deck Environment

LSO Display Workstation

LSO Windscreen

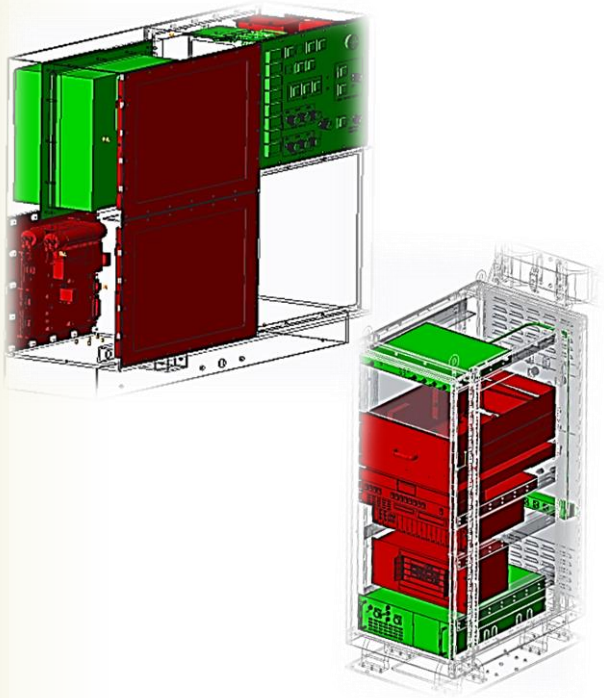


Base Console

Below Deck Equipment Room Exists as well

Distribution: LSODS Case Study

Critical Components



100s of Parts

Drawing	CAGE	Mfg	Assembly & Part Description	Part Number	FSC	NIIN	CAGE	MFG & or P/N Notes	Available	Notes
4099A55070-st	30003		DUAL FAN PANEL ASSY							
			WASHER, FLAT, REDUCED OD.	NAS620C8L	5310	01-627-9283				
			PAN HEAD SCREW	MS51957-46	5305	00-054-6671				
			NUT	MS35649-284	5310	00-934-9759				
			LOCK WASHER	MS35338-137	5310	00-933-8119				
			TERMINAL LUG	MS17143-10	5940	00-825-3699		TE 2-327950-1	YES	
			TERMINAL BLOCK, NAVY CLASS	8TB2	5940	00-500-5388	26405	MARATHON SPECIAL PRODUCTS	YES	
	052W9	MECHATRONICS FANS GROUP	FAN GUARD	SGR-59	4140	01-614-7276	052W9	MECHATRONICS, INC.	YES	
	*06383	Panduit	CABLE CLAMP	LWC25-A-C14		No NIIN	06383	Panduit	YES	
	*00779	TE / Raychem	LABEL, CABLE MARKING, 3/32" ID	TMS-SCE-3/32-2.0-9	5970	01-465-4153	06090	TE	YES	
4099A55073-1	30003	Parker Hannifin	PANEL, AIR VENT-EMI	06-0302-12404	1680	01-655-9866	18565	Parker Hannifin		781-935-4850
4099A55072-1	30003	HAMMOND MFG CO U S INC	FAN PANEL, DDCP	PBPA1901UNF		No NIIN	4F708	Hammond		
4099A55071-1	30003	MECHATRONICS FANS GROUP	AXIAL FAN, AC	UF15KC12-BWHR	1680	01-655-9865	052W9			
628080	30003		DUAL FAN PANEL ASSY , DDCP							
4099A55080	30003		SPEED CONTROLLER ASSEMBLY, DDCP							
			NUT, PLAIN .190-32 UNF							
			WASHER, FLAT, REDUCED OD.							
			WASHER, FLAT, REDUCED OD.							
			PAN HEAD SCREW							
			PAN HEAD SCREW							
			NUT							
			LOCK WASHER							
			LOCK WASHER							
			TERMINAL LUG	MS17143-10						
			TERMINAL BLOCK, NAVY CLASS	8TB2	5940	00-500-5388	26405	MARATHON SPECIAL PRODUCTS		
	0YAN7	CONTROL RESOURCES INC.	CONTROLLER, FAN SPEED	240B3W00-F						
		Tyco / TE	LABEL, CABLE MARKING, 1/8" ID	MS-SCE-1/8-2.0-9						
			BRACKET, FAN SPEED CTRL							
425511	80020	Cutler-Hammer (Eaton)	Limit Switch	6894ED64-36			27191			
518924-1	80020 (90129)	Joy Manufacturing	Pendant Switch (Hydraulic Lifting Unit)							
518925R-S1										

	A	D	F	G	H	I	L	M
1	NAWCAD Part Number	Primary Vendor Part NO.	Description	CAGE CODE	Manufacturer	Good known part & available	FSC	NIIN
167	A218415-167	No Item Listed						
168	A218415-168	E-62H	Retaining Ring		CAPLUGS			No NIIN
169	A218415-169	No Item Listed						
170	A218415-170	C0975-105-3000-S			Associated Spring-Raymond	Yes		No NIIN
171	A218415-171	No Item Listed						
172	A218415-172	No Item Listed						
173	A218415-173	H-9174			Bud Industries	Yes		
174	A218415-174	FHS-632-10	STUD,SELF-LOCKING	46384	Penn Engineering		5307	01-374-2314
175	A218415-175	LAC-632-2F	NUT,SELF-LOCKING,CLINCH	46384	Penn Engineering		5310	00-873-3195
176	A218415-176	LAC-0420-2F	NUT,SELF-LOCKING,CLINCH	46384	Penn Engineering		5310	00-956-5435
177	A218415-177	CLS-440-3	NUT,PLAIN,CLINCH	46384	Penn Engineering		5310	00-800-0074
178	A218415-178	CLS-832-3	NUT,PLAIN,CLINCH	46384	Penn Engineering		5310	00-725-8532
179	A218415-179	No Item Listed						
180	A218415-180	CMZ10-IBM	CABLE ASSEMBLY,SPECIAL ELECTRICAL	43321	L-Com	Yes	5995	01-611-9922
181	A218415-181	CTL1B-5	CABLE ASSEMBLY,POWER,ELECTRICAL	43321	L-Com	Yes	6150	01-531-5473
182	A218415-182	CTL1B-15			L-Com	Yes		No NIIN
183	A218415-183	TRD8555Z-5	CABLE ASSEMBLY,SPECIAL,ELECTRICAL		L-Com	Yes	6150	01-518-4197
184	A218415-184	TRD8555Z-7	CABLE ASSEMBLY,SPECIAL,ELECTRICAL		L-Com	Yes	6150	01-516-6492
185	A218415-185	TRD8855Z-1			L-Com			No NIIN
186	A218415-186	88741-8120	CABLE,DVI-DVI,AIRCR	27264	Molex		1710	01-531-5475
187	A218415-187	SPC13298	D-Sub Connector		Multicomp	Yes		No NIIN
188	A218415-188	SPC13300	D-Sub Connector		Multicomp	Yes		No NIIN
189	A218415-189	17273A			Volex	Yes		No NIIN
190	A218415-190	88741-8100	CABLE ASSEMBLY,RADIO FREQUENCY	1UX99	Molex		5995	01-586-5945
191	A218415-191	31-4803-1101	ADAPTER,CONNECTOR	77820	Amphenol	Yes	5935	01-432-0480
192	A218415-192	No Item Listed						
193	A218415-193	No Item Listed						
194	A218415-194	No Item Listed						
195	A218415-195	No Item Listed						
196	A218415-196	No Item Listed						

74323 DVI

SPC13298

SPC13300

74323 DVI

Distribution: LSODS Case Study

- Government serves as LSI
- Fielded on all Carriers, including Ford Class
- Originally Designed in 1980s
- No Program Protection Plan (Not required at time of MSDs)
- Future installs will require New Hardware Buys (ECP Approved for config changes)
- Components supplied via requisition NAVSUP/DLA COTS
- No vendors/Long Term Contracts for repair/manufacture in place

Distribution: QUESTIONS

How much visibility into DLA/NAVSUP fulfillment lines are necessary (not LSODS specific)?

What should a Government Product Support Team know about DLA/NAVSUP fulfillment lines?

If going to vendor directly (Or vendor providing), how much visibility is needed?

When does criticality matter for Distribution Channels?

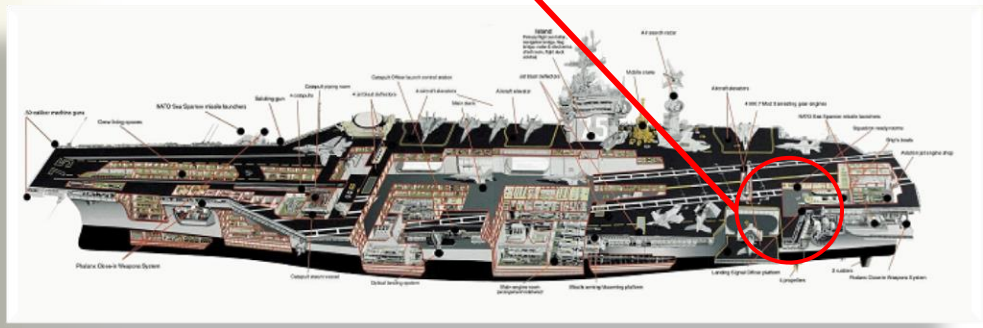
What Distribution Information do we want available?

Where can Industry help?

If an OEM serves as an LSI, do these answers change?

IT/Cyber in Supply Chain for Surety Breakout Group

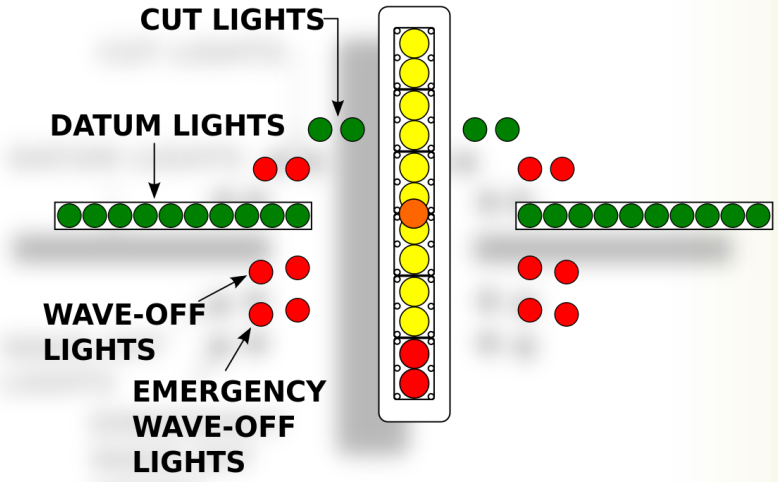
IT/Cyber: IFLOLS Case Study

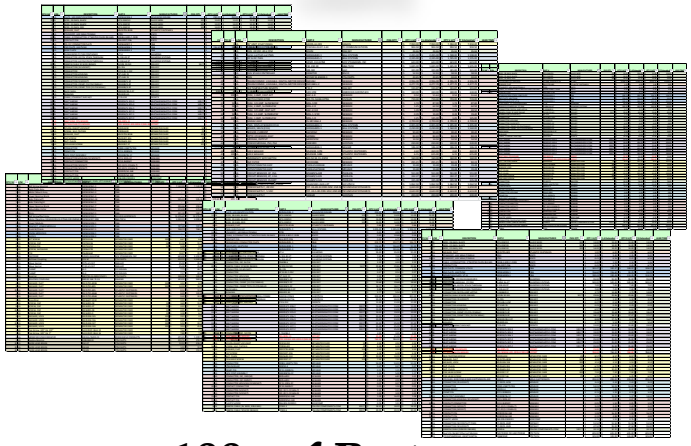


- Improved Fresnel Lens Optical Landing System (IFLOLS)
- Pilots use IFLOLS to discern glide slope—the angle at which aircraft descend and land—by tracking the up-and-down motion of a "meatball," a bright amber light. The more closely aligned the meatball is with a horizontal row of green "datum" lights, the closer an aircraft is to its prescribed glide slope.

IFLOLS Case Study

- IFLOLS has over 760 line items
- Approximately 70 different manufacturers supply components
- MOUSER Electronics is one of 70 different companies that provide parts for IFLOLS
- MOUSER Electronics maintains relationships with more than 750 manufacturers worldwide
- MOUSER has 22 locations located strategically around the globe





100s of Parts

IFLOLS Case Study

- Do we need a toolset for tracking efforts?
  - Where does the tool reside? Program office?
  - Industry? Does Navy need visibility?
- What should the toolset tell us?
- Is this something we should be tracking?
- How do we maintain visibility of all manufacturers?
  - Do we need to maintain visibility?
  - Does industry maintain visibility?

Back up

"Counterfeits Continue to Pose Risk to US Navy"

Counterfeits

INCIDENT:

In October of 2015, a Massachusetts man was sentenced for importing thousands of counterfeit integrated circuits (ICs) from China and Hong Kong and reselling them to U.S. customers, including contractors supplying them to the U.S. Navy for use in nuclear submarines. Picone admitted that he resold the counterfeit ICs to customers both in the United States and abroad, including to Defense contractors that Picone knew intended to supply the counterfeit ICs to the U.S. Navy for use in nuclear submarines, among other things.

IMPACT:

Picone admitted that he knew that malfunction or failure of the ICs likely would cause impairment of combat operations and other significant harm to national security.

The potential risk of counterfeit routers, servers, or other hardware and software are potentially catastrophic for Defense customers. "Counterfeit electrical components intended for use in U.S. military equipment put our service members in harm's way, and our national security at great risk," said a special agent involved in the case.

MITIGATION:

Picone pleaded guilty on June 3, 2014, to conspiracy to traffic in counterfeit military goods. On October 6, 2015, he was sentenced to 37 months in prison. In addition, Picone has been ordered to pay $352,076 in restitution to the 31 companies whose ICs he counterfeited, and to forfeit $70,050 and 35,870 counterfeit ICs.

- https://www.govtechworks.com/counterfeit-tech-marks-another-front-for-security-vigilance/
- http://www.justice.gov/opa/pr/massachusetts-man-sentenced-37-months-prison-trafficking-counterfeit-military-goods-0

"Obsolete Electronic Parts Sold to U.S. Military"

Counterfeits

INCIDENT:

On July 28, 2015, Jeffrey Krantz, CEO and owner of Harry Krantz, LLC, was charged and pleaded guilty to wire fraud for his role in the sale of unapproved aircraft parts. Harry Krantz, LLC, bought and sold obsolete electronic parts for ultimate use by commercial buyers and the U.S. Military.

Krantz knew that the chips had originated from a parts supplier in China, and there was a high probability that the chips were falsely remarked and not the original chips of the certain manufacturer as represented by the markings on the chip. He also avoided engaging in common practices in the industry to avoid confirming that the chips were likely remarked.

IMPACT:

The investigation revealed that many of the chips were used in the assembly of U.S. Military and commercial helicopters. The chips have been examined and determined not to be the root cause of any mechanical problems experienced by the helicopters to date.

"The distribution of unapproved microprocessor chips and other electronic components for use by the U.S. Military poses a serious threat to the safety of the men and women of our armed services," said U.S. Attorney Daly.

MITIGATION:

Law enforcement continues to have a major challenge in getting the prosecutors to understand the seriousness of these counterfeit electronic component crimes and why the behavior of so many companies is truly unacceptable and must change.

Krantz has agreed to pay restitution in the amount of $402,650. He also has agreed not to be directly or indirectly involved in the buying or selling of electronic parts, for a period of up to two years, and to give up all control either directly or indirectly over Harry Krantz LLC, and all beneficial and/or financial interest, including ownership interest, in Harry Krantz, LLC and will not reacquire such an interest.

- https://www.linkedin.com/pulse/ceo-harry-krantz-sentenced-wire-fraud-well-almost-dan-matis?trk=pulse-det-nav_art
- https://www.oig.dot.gov/library-item/32595
- http://www.justice.gov/usao-ct/pr/new-york-man-admits-supplying-falsely-remarked-computer-chips-used-us-military

“Chinese Hackers Target Logistics and Shipping Firms With Poisoned Inventory Scanners”

Hardware

INCIDENT:

In a cyberattack campaign dubbed “ZombieZero,”a popular brand of Chinese manufactured inventory scanners that contained preloaded malware stole sensitive information from shipping and logistics companies. According to TrapX Security, an unnamed Chinese manufacturer implanted malware into its handheld terminal scanners and in software updates available for download on its support website. They delivered the infected devices to customers where the scanners launched an automated attack that sent inventory information to botnets in China, and downloaded additional malware that infiltrated corporate servers and targeted sensitive financial and customer information.

IMPACT:

The Chinese manufacturer sells handheld scanners to companies around the world. The exact amount of affected companies is unclear, but the manufacturer recently delivered infected scanners to 7 logistics and shipping companies and 1 large robotics manufacturing firm. One affected company was running 16 infected scanners that compromised 9 of its corporate servers. According to TrapX, the attackers successfully stole all financial and customer data, which can provide the attackers complete situational awareness and visibility into the company’s operations.

MITIGATION:

The attack was discovered when a TrapX solution was deployed in the victim company’s environment as part of a proof-of-concept. The solution immediately detected the attack, reported its anatomy and performed a complete automated forensic analysis.

http://www.darkreading.com/attacks-breaches/chinese-hackers-target-logistics-and-shipping-firms-with-poisoned-inventory-scanners/d/d-id/1297182
http://www.scmagazineuk.com/china-accused-of-global-zero-day-attack-on-shipping-firms/article/360406/
http://www.trapx.com/wp-content/uploads/2014/07/TrapX_ZOMBIE_Report_Final.pdf

“Drone Developed That Hacks Unsecure Computer Networks”

Hardware

INCIDENT: During DEFCON 2015, Aerial Assault revealed a drone that can swoop down and break into computer networks. On board the drone, an ultra-cheap Raspberry Pi computer runs Kali Linux, an aggressive cybersecurity diagnostic tool that looks for weaknesses in the systems it attacks. Set up as a security testing tool, with some reconfiguring it could go from a testing device to an actual weapon.

Reportedly, the drone will retail for $2,500, which is on the upper end for hobbyist drones but advertised as within the budgets of businesses or government buyers.

IMPACT: The Aerial Assault drone looks for unsecured networks, and using its onboard GPS it records the locations of the targets and relays that information back to the remote pilot. The pilot can then decide whether to use Kali Linux to hack into the network's servers.

A previous version of the drone featured its own WiFi signal, enabling the users to trick laptops, phones and other devices in an area to connect to his drone rather than a trusted network. That would have made it easier for hackers to sweep up data that passes through the connection, including credit card numbers, banking information and the like.

MITIGATION: According to the developer, “There has never been this capability before.” Consequently, mitigations are unknown.

- http://www.popsci.com/drone-defcon-hacks-sky
- http://www.ibtimes.com/aerial-assault-drone-helps-hackers-penetrate-internet-networks-sky-2046283

"Outsiders Access Japanese Nuclear Reactor Control Room Data"

Software

INCIDENT:
In January 2014, it was determined that hackers may have stolen private information from one of the eight computers in the reactor control room at the Monju fast-breeder reactor offices. For 5 days starting on December 26, 2013, the computer, which stores more than 42,000 e-mails and staff training reports, had been accessed more than 30 times with the requests coming from a website based in South Korea. A server administrator discovered that the malware infected the computer after an employee updated free software that was installed on the computer.

IMPACT:
Since the computer is only used by workers to file paperwork, the damage that the malware could have caused is limited. However, after finding traces of out-bound transmissions, investigators concluded that the cybercriminals controlling the malware could have stolen sensitive documents, including emails, training records and employee data sheets.

MITIGATION:
The Japan Atomic Energy Agency (JAEA) currently is investigating how the infection occurred and identifying the data on the computer that could have been accessed. In November 2013, the agency had been warned by the country's nuclear regulator that its anti-terrorism measures were not up to snuff. "The regulatory agency rebuked the JAEA for violating security guidelines meant to protect nuclear materials from terrorism and other malicious attacks," Enformable reported.

- http://www.nextgov.com/cybersecurity/threatwatch/2014/01/breach/689/
- http://enformable.com/2014/01/computer-control-room-monju-fast-breeder-reactor-infected-virus/

"The Hacker Who Worked on a Navy Nuclear Aircraft Carrier"

Software

INCIDENT:

Nicholas Knight, a former system administrator who supported the USS Harry Truman's nuclear reactor department, led a hacktivist group called Team Digi7al and carried out hacks while on active duty, even using the Navy's network.

Throughout 2012, the group exploited SQL vulnerabilities to attack largely government-related sites including NGA, DHS, the Toronto Police Department, and the Navy to gather sensitive and private information and publically disclose it on Twitter.

IMPACT:

According to court documents, the group accessed schematics for more than ten NGA databases, breached the DHS-TWIC (Transportation Worker Identification Credential) database that houses sensitive biometric data for credentials, and stole the names and addresses of more than 500 confidential police informants from the Toronto police department.

The group also stole an unknown amount of personal records from the Navy Smart Web Move (SWM) site, which manages military personnel transfers for more than 220,000 military members and families. This breach also caused a premature shutdown of the site that lasted 10 weeks disrupting logistical operations and causing $514,000 in damages.

MITIGATION:

A Naval Criminal Investigate Service (NCIS) investigation into the SWM hack revealed Team Digi7al's extensive computer hacking scheme and led to the arrest of Knight and another member of Team Digi7al. Knight was discharged from the Navy in 2012 after being caught attempting to hack a Navy database while onboard a Navy vessel.

The two Digi7al members are awaiting trial and could face up to five years in prison, a $250,000 fine, and restitution to any victims.

http://www.wired.com/wp-content/uploads/2014/05/Nicholas-Knight1.pdf
http://www.wired.com/2014/05/navy-sysadmin-hacking/
http://www.justice.gov/usao/okn/news/2014/teamdigi7al0505.html

"U.S. Files Criminal Charges Against Chinese Military Hackers Over Cyber Espionage"

Software

INCIDENT:

Five soldiers from a secret Chinese military cyber unit, known as Unit 61398 of the Third Department of the Chinese People's Liberation Army, hacked at least six American companies as part of an ongoing economic espionage campaign. The hackers allegedly breached the networks of U.S. nuclear power, metals and solar product companies and maintained unauthorized access for nearly eight years while stealing intellectual property, sensitive internal communications, and confidential business information.

IMPACT:

According to the indictment, the hackers stole confidential cost, pricing and strategy information; sensitive internal communications regarding China-U.S. trade litigations and labor disputes; and proprietary technical and design specifications. This information gives Chinese competitors, including state-owned enterprises, an unfair economic advantage and enables them to target business operations of U.S. companies aggressively from a variety of angles. It also sabotages American companies and undermines the integrity of fair competition in the operation of the free market.

MITIGATION:

Following an FBI investigation that traced the attacks to Unit 61398's Shanghai headquarters, the Justice Department filed criminal chargers against five soldiers from the unit for computer hacking, economic espionage and other offenses. A grand jury in the Western District of Pennsylvania indicted the five military hackers charging them each with 31 criminal counts.

In a public statement, Alcoa claimed that "no material information was compromised during this incident…" and that they would continue to invest resources to protect their system as safeguarding their data is a top priority.

http://www.justice.gov/opa/pr/2014/May/14-ag-528.html
http://www.nbcnews.com/news/us-news/u-s-charges-china-cyber-spying-american-firms-n108706
http://www.cbsnews.com/news/u-s-government-files-economic-espionage-charges-against-chinese-hackers-sources-say/

“Software Vulnerability Unlatches Car Doors and Unhinges Automobile Manufacturers”

Software

INCIDENT:

Land Rover has recalled over 65,000 vehicles worldwide sold between 2013 and now. This recall is to fix a software bug that is capable of “unlatching” the vehicles’ doors. It speculated that thieves are able to use a “black box” device to unlock cars that have keyless ignitions. Blank keys can then be used to steal the vehicle. Other targeted vehicles include the BMW X5, Ford Fiesta, Ford Focus and certain Audi models.

IMPACT:

The software vulnerability has already caused an increase in stolen vehicles, but the security flaw is causing other problems for car owners. Insurance companies are refusing to cover Land Rover owners unless they can prove that they are able to park in secure lots that are off of the street. The vulnerabilities associated with these vehicles are allowing thieves to steal-to-order and sell stolen vehicles to chop shops.

MITIGATION:

Land Rover has already recalled over 65,000 vehicles in order to patch this security flaw. All vehicles with keyless entry and ignition systems have the potential for vulnerabilities and flaws. Therefore, all major automobile manufacturers are working to find a solution to the vulnerabilities associated with keyless entry and ignition.

- http://www.bbc.com/news/technology-33506486

"Car Vulnerability Allows Hackers to Remotely Access and Control Moving Vehicle"

Software

INCIDENT:

In July 2015, hackers demonstrated their ability to remotely access and control a moving vehicle. Though the driver of the Jeep Cherokee was expecting this, as he had agreed to be part of the experiment, he was startled when the Jeep's transmission was disengaged remotely, rendering him unable to move on a busy highway.

IMPACT:

The hackers were able to control the vehicle through a vulnerability in the Wi-Fi system that is implemented in the car. They were able to control the vehicle's windshield wipers, air conditioning, radio and even made themselves appear on the dashboard console.

MITIGATION:

Chrysler has been working to fix the vulnerability. Chrysler has created a patch that should fix the vulnerability, but it must be manually implemented. Additionally, actions taken by the Senate may lead to security standards across the entire automotive industry.

- http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway
- http://www.wired.com/2015/07/senate-bill-seeks-standards-cars-defenses-hackers/

"Russian Programmers Coding for US Military Systems"

Software

INCIDENT: The Pentagon was tipped off in 2011 by a longtime Army contractor that Russian computer programmers were helping to write computer software for sensitive U.S. military communications systems. The contractor, John C. Kingsley, said in court documents filed in the case that he discovered the Russians' role after he was appointed to run one of the firms in 2010. Greed drove the company to employ the Russian programmers, he said in his March 2011 complaint. He said they worked for one-third the rate that American programmers with the requisite security clearances could command. His accusations were denied by the firms that did the programming work.

IMPACT: In court documents, Mr. Kingsley said the software had made it possible for the Pentagon's communications systems to be infected with viruses. "On at least one occasion, numerous viruses were loaded onto the Defense Information Systems Agency (DISA) network as a result of code written by the Russian programmers and installed on servers in the DISA secure system," Kingsley said in his complaint, filed under the federal False Claims Act in U.S. District Court in Washington, D.C., on March 18, 2011.

Asked to confirm that the Russians' involvement in the software work led to the presence of viruses in the U.S. military's communications systems, a spokeswoman for DISA, declined to answer on the grounds that doing so could compromise the agency's "national security posture."

MITIGATION: The incident set in motion a four-year federal investigation that ended with a multimillion-dollar fine against two firms involved in the work. NetCracker and the much larger Virginia-based Computer Sciences Corporation—which had subcontracted the work—agreed to pay a combined $12.75 million in civil penalties to close a four-year-long Justice Department investigation into the security breach.

The agency's inspector general, Col. Bill Eger, who had investigated Kingsley's allegations, said the case was a good example of how his office combats fraud. In a separate statement, the U.S. Attorney for the District of Columbia, said that "in addition to holding these two companies accountable for their contracting obligations, this settlement shows that the U.S. Attorney's Office will take appropriate measures necessary to ensure the integrity of government communications systems."

- http://www.thedailybeast.com/articles/2015/11/04/pentagon-farmed-out-its-coding-to-russia.html#
- http://www.publicintegrity.org/2015/11/04/18828/security-breach-russian-programmers-wrote-code-us-military-communications-systems
- https://fcw.com/articles/2015/11/05/contracting-fines-russian-programmers.aspx

"Widespread Neglect Puts NASA's Networks in Jeopardy"

Software

Common Development Practice:

The National Aeronautics and Space Administration (NASA) is in serious risk of a cyber attack according to recent reports. Internal documents indicate that NASA has anywhere from hundreds of thousands to millions of out-of-date patches at every data center in the country. Hewlett Packard Enterprise, who holds a $2.5 billion dollar IT contract with NASA, is said to be uncooperative at best and negligent at worst, failing to keep up with mandatory patching required by the contract.

Experts say NASA is as vulnerable today as Office of Personnel Management (OPM) was before it was attacked. The chief operating officer and co-founder of Security Scorecard said the malware activity coming from NASA is astonishing. He continued to say that some of these malware families are some of the most malicious known viruses in existence.

Operational Impact:

The co-chairman of NASA Labor-Management Forum explains that they are committed to continuing to urge NASA leadership to enhance NASA's IT security posture and to ask Congress to increase funding for this important priority. Since the arrival of a new Chief Information Officer (CIO), this backlog has been significantly reduced and NASA is continuing to work this issue. However, the issue has not been resolved and NASA has a long way to go.

Risk:

The missing patches could open the door for a hacker to take over privileged administrative rights, and could let a hacker execute malware through a commonly used software title, meaning they are behind the firewall and other external cyber defenses with little effort.

Security Scorecard, a cybersecurity company, found up to 10,000 pings in NASA's networks from known malware hosts. Some lasting for months.

- http://federalnewsradio.com/cybersecurity/2016/03/widespread-neglect-puts-nasas-networks-jeopardy/

“Chinese National Charged for Stealing Source Code from Former Employer with Intent to Benefit Chinese Government”

Software

INCIDENT:
According to allegations coming from the US Department of Justice Assistant Attorney General, a Chinese National “allegedly stole proprietary information from his former employer for his own profit and the benefit of the Chinese government.” The proprietary software is a clustered file system developed to facilitate faster computer performance by coordinating work among multiple servers.

The Chinese National worked as a developer for a U.S. company and was able to obtain the proprietary software during his time with that company. The code was only accessible to a small subset of the company’s employees.

IMPACT:
The Chinese National duplicated and possessed the proprietary source code that helps a computer's performance by coordinating work among multiple servers with the intent to benefit himself and the National Health and Planning Commission of the People’s Republic of China.

MITIGATION:
The Chinese National was caught by two undercover law enforcement officers who posed as potential buyers of the proprietary software.

Following his arrest the man was charged with six counts of economic espionage and theft of trade secrets. The case is being investigated by the Federal Bureau of Investigation (FBI) and is being prosecuted by the National Security division’s Counterintelligence and Export Control Section.

Each of the three counts of espionage carry a maximum sentence of 15 years in prison. The three counts of theft of a trade secret each carry a maximum sentence of 10 years in prison.

- https://www.justice.gov/opa/pr/chinese-national-charged-stealing-source-code-former-employer-intent-benefit-chinese
- http://www.bbc.com/news/business-36535577

“Hollywood Hospital Pays Ransom to Hackers”

Services

INCIDENT:
On February 5, 2016, the Hollywood Presbyterian Medical Center fell victim to a malware attack that affected the enterprise-wide hospital information system. The malware locked systems by encrypting files and demanding ransom to obtain the decryption key. On February 15, 2016, the HPMC restored its electronic medical record system (EMR) and full operability.

IMPACT:
The malware denied access to certain computer systems and prevented the hospital from sharing communications electronically. Staff were forced to carry out some tasks on paper. Chief Executive Allen Stefanek said patient care was never compromised, nor were hospital records.
Although ransomware attacks are rare, cyber attacks on medical centers are becoming more frequent as hackers attempt to gain personal information for fraud schemes.

MITIGATION:
In order to obtain the decryption key from the hackers and release the files, the Hollywood Presbyterian Medical Center paid the ransom of 40 bitcoins, or about $17,000. All systems currently in use were cleared of the malware and thoroughly tested.
The hospital continues to work with their team of computer experts and law enforcement to understand more about the event.

- http://www.bbc.com/news/technology-35602527
- http://hollywoodpresbyterian.com/default/assets/File/20160217%20Memo%20from%20the%20CEO%20v2.pdf
- http://www.latimes.com/business/technology/la-me-ln-hollywood-hospital-bitcoin-20160217-story.html

“Home and Office Air Conditioners Able to Hack Power Grid”

Services

IoT CAPABILITY:

In February 2016, international researchers found a way to take down the power grid by remotely manipulating home and office air conditioners, creating a surge during peak energy periods and widespread blackouts.

The hackers target remote shut-off devices that utility companies install on air conditioners. During normal operations, regional power centers can send a command via radio frequency to reach devices and shut down air conditioners. However, because the companies do not use encryption or authentication, anyone in the vicinity who can emit a stronger signal than the one the utility company can manipulate the devices as well.

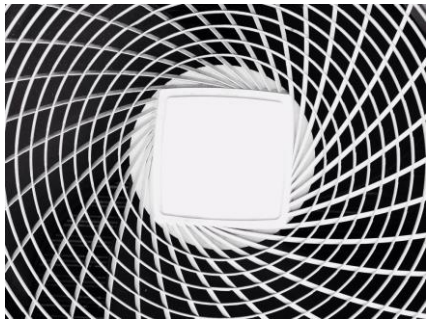
IMPACT:

The vulnerability reveals the ability to cut air conditioners during a heatwave—creating a potentially fatal condition for the elderly and sick.

Furthermore, research reveals that a more widespread blackout could occur if an attacker were to turn the air conditioners on and off repeatedly, creating disturbances and imbalances in the grid that could trip breakers beyond the neighborhood they are targeting.

MITIGATION:

The two researchers, from Kaspersky Lab and Exigent Systems, would not identify the devices they examined since they are still in the process of reaching out to vendors. However, one researcher says that the chips used in some of them are so outdated and limited—one system they examined used a chip made in 1995—that even if the vendors wanted to add authentication to make the devices more secure he doubts they could do it, raising additional concerns for power grid security.



- http://www.wired.com/2016/02/how-to-hack-the-power-grid-through-home-air-conditioners/

Question Review

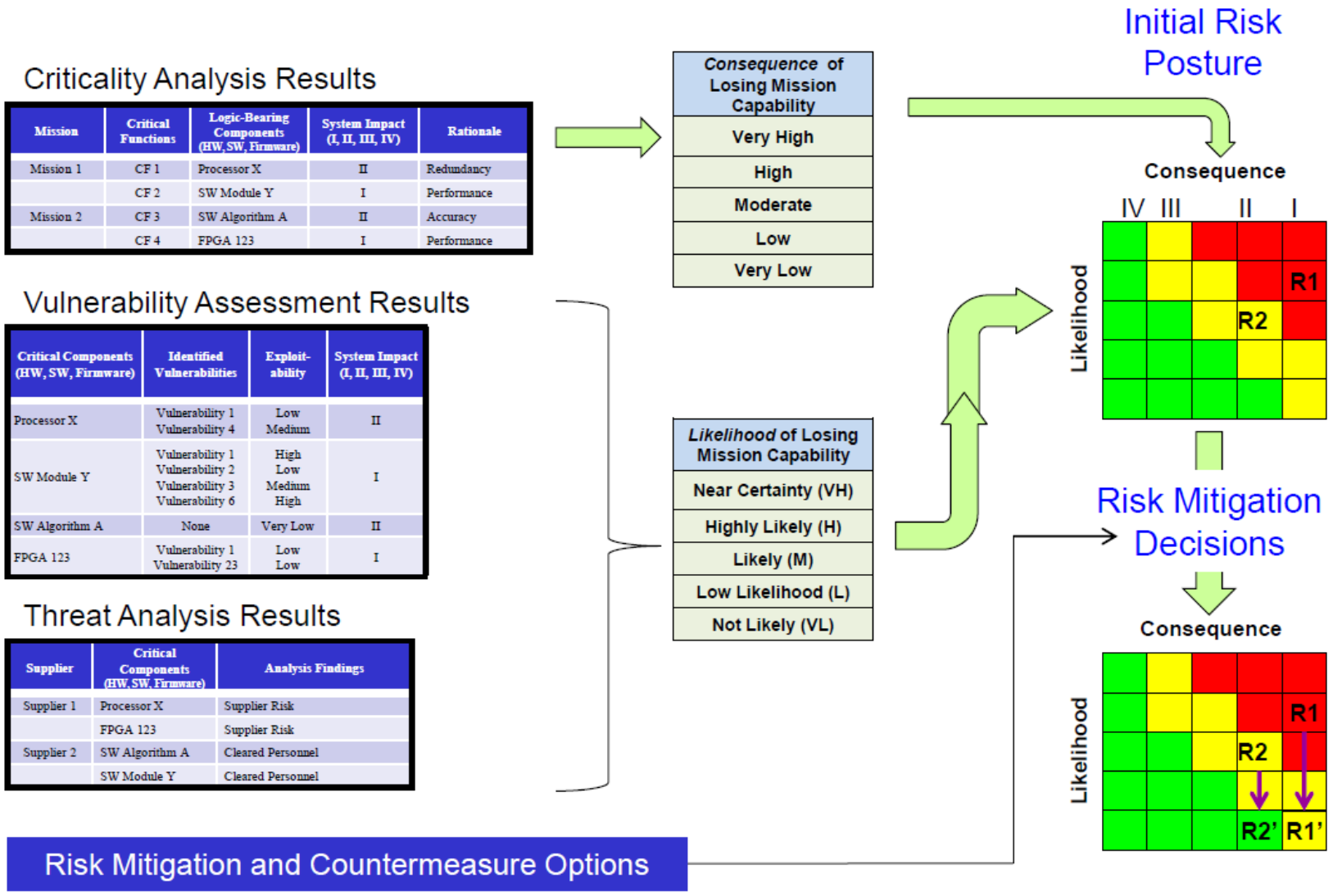
- What are the risks and who is responsible? Prioritize risks (how?) How do you manage this risk?
- Strategies to mitigate risk? Are the current Navy efforts enough? What should we be doing that we are not doing? How do we implement these measures?
- What are some mitigating strategies? Is there a way to monitor this?
- How can Navy assist? Navy/Industry collaboration?
- Where are the gaps/vulnerabilities?
- How do we monitor? What are the metrics? How do we incentivize industry?
- What is the role of industry?

What is Asked in a PPP?

- **Supply Chain Risk Management**
- How will the program manage supply chain risks to CPI and critical functions and components?
- Explain how supply chain threat assessments will be used to influence system design, development environment, and procurement practices. Who has this responsibility? When will threat assessments be requested?
-
  - ***Trusted Suppliers***
- Will any ASICs require trusted fabrication?
- How will the program make use of accredited trusted suppliers of integrated circuit-related services?
  - ***Counterfeit Prevention***
- What counterfeit prevention measures will be in place? How will the program mitigate the risk of counterfeit insertion during Operations and Maintenance?

Extracted from www.acq.osd.mil/se/docs/PPP-Outline-and-Guidance-v1-July2011.docx

SCRM Methodology



Criticality Levels from PPP

Level I – Total Mission Failure	Function/component failure results in total compromise of mission thread
Level II – Significant/Unacceptable Degradation	Function/component failure results in unacceptable compromise of mission thread or significant mission degradation
Level III – Partial/Acceptable	Function/component failure results in partial compromise of mission thread or partial mission degradation
Level IV – Negligible	Function/component failure results in little or no compromise of mission thread

Timeline to Industry Day