Preserving Product Data Integrity: Securing the Supply Chain

THE VALUE OF PERFORMANCE.

NORTHROP GRUMMAN

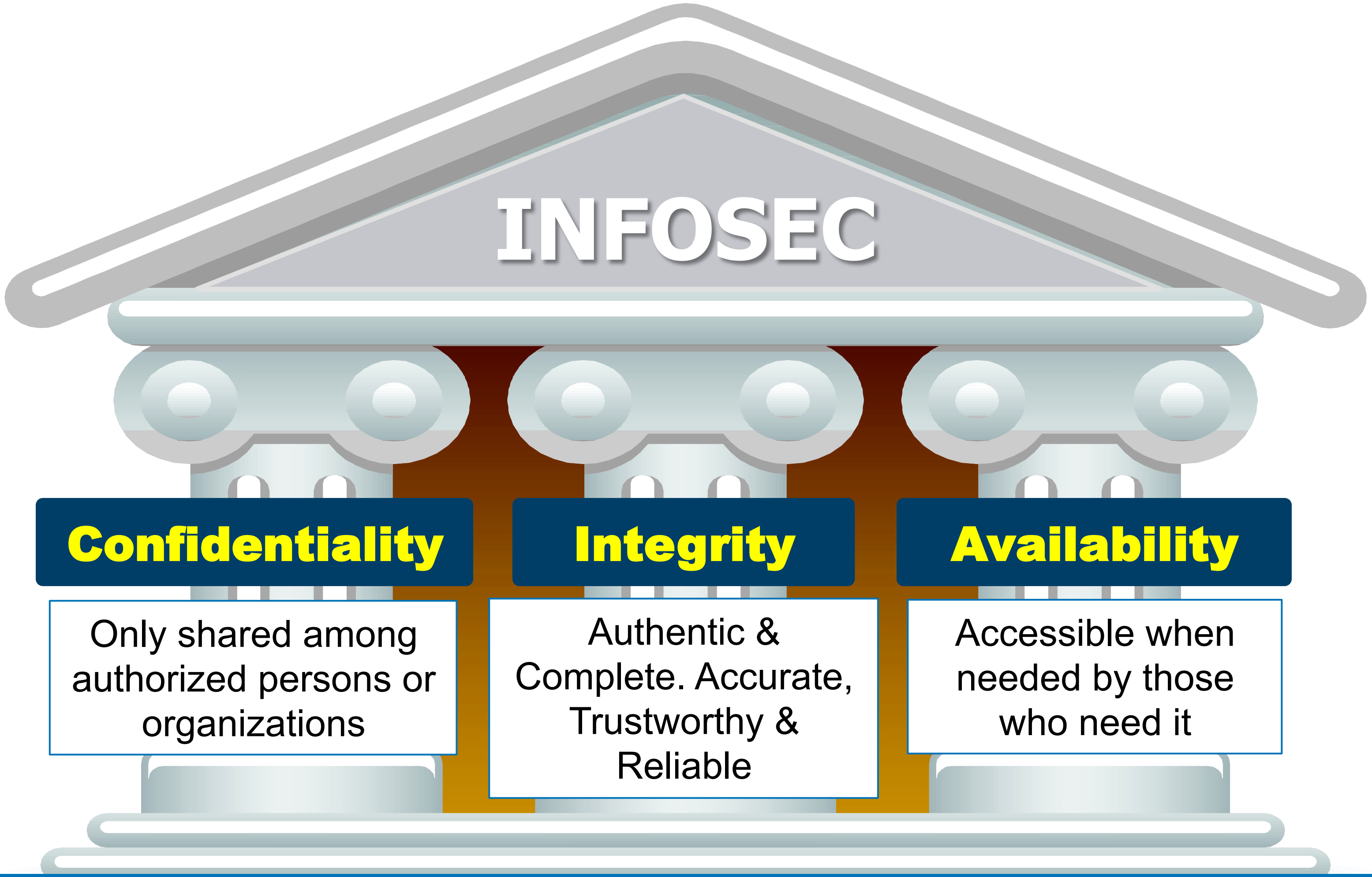
2014 GPDIS

9 September 2014

Mike Papay
Vice President
Chief Information Security Officer
Northrop Grumman Corporation

Approved for public release Case # 14-1805

The Three Pillars of Information Security: CIA Triad



INFOSEC

Confidentiality

Only shared among authorized persons or organizations

Integrity

Authentic & Complete. Accurate, Trustworthy & Reliable

Availability

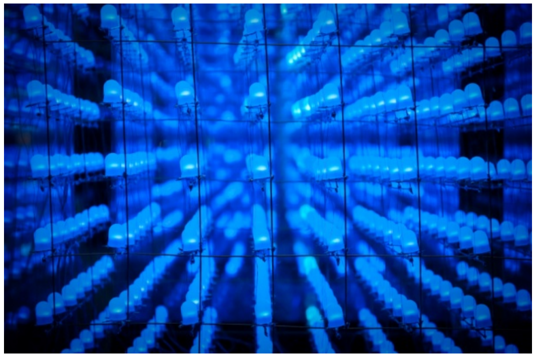
Accessible when needed by those who need it

Security Controls are measures taken to safeguard the *Confidentiality*, *Integrity*, and *Availability* of a system and its information

Definitions from NIST 800-53r4. http://dx.doi.org/10.6028/NIST.SP.800-53r4

Lights

- First rule of securing your system against cyber threats and supply chain attacks?



- Check out all the lights that are blinking
  - **Know** what you've got to protect!
  - **See** what all those blinking lights do
  - **Document** everything so you can manage it
- **Shine a light** on your success stories
- **Light a fire** under your employee training process
  - Many acquisition professionals want to learn about cyber
  - Cyber techniques and technologies can be applied almost anywhere

Camera

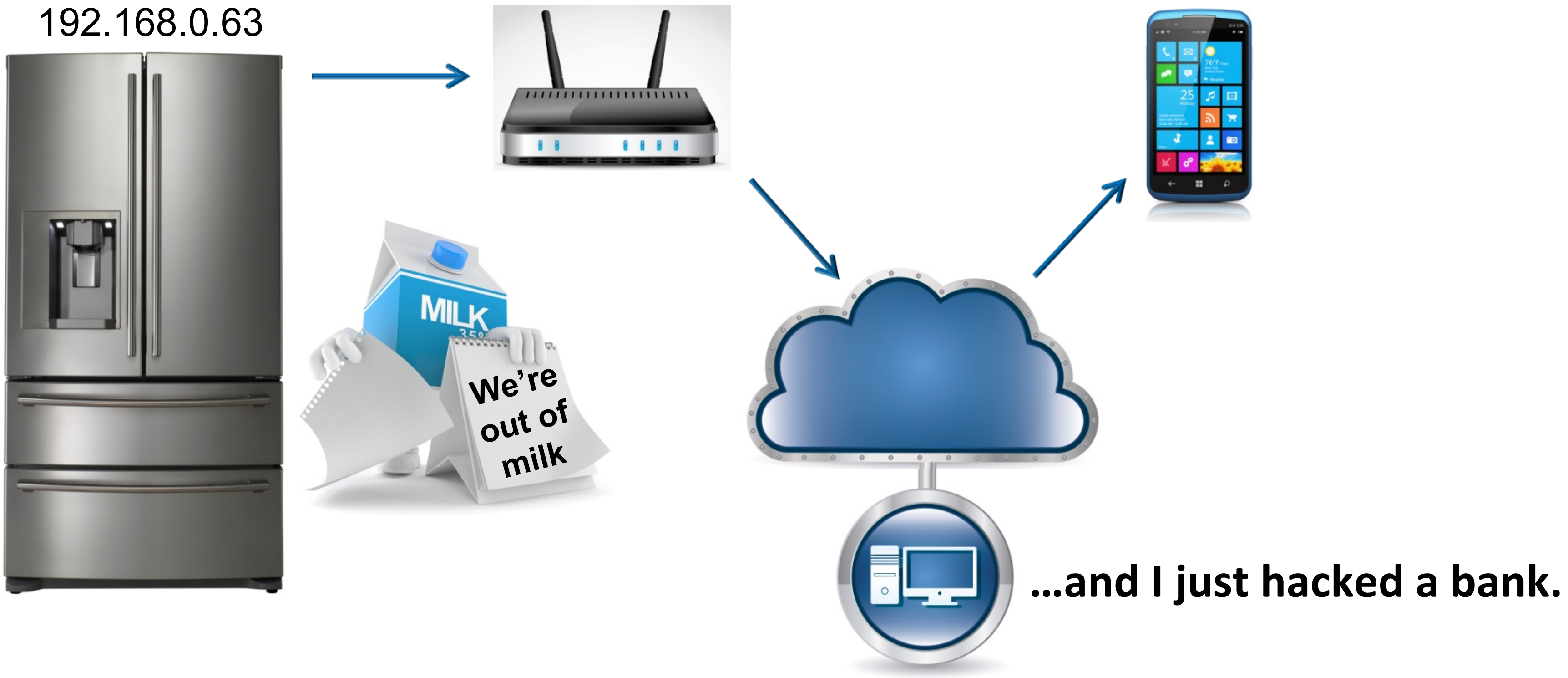
- Set up your systems so you can record everything that occurs
  - **Inbound:** watch for malware and other attacks
  - **Outbound**: watch for exfiltration
  - **Internally**: watch for anomalies

- If you are considering a move to the cloud, make sure you have the same control over that cloud that you do internally

- What do we do with all this data we’re recording?!
  - **Store** what you can afford
  - **Analyze** what you need
  - **Visualize** the things that are important to you

Action

- Continuously improve your IT architecture with security in mind
  - Think: “Secure by Design”
- The Internet of Things (and a lesson for us)

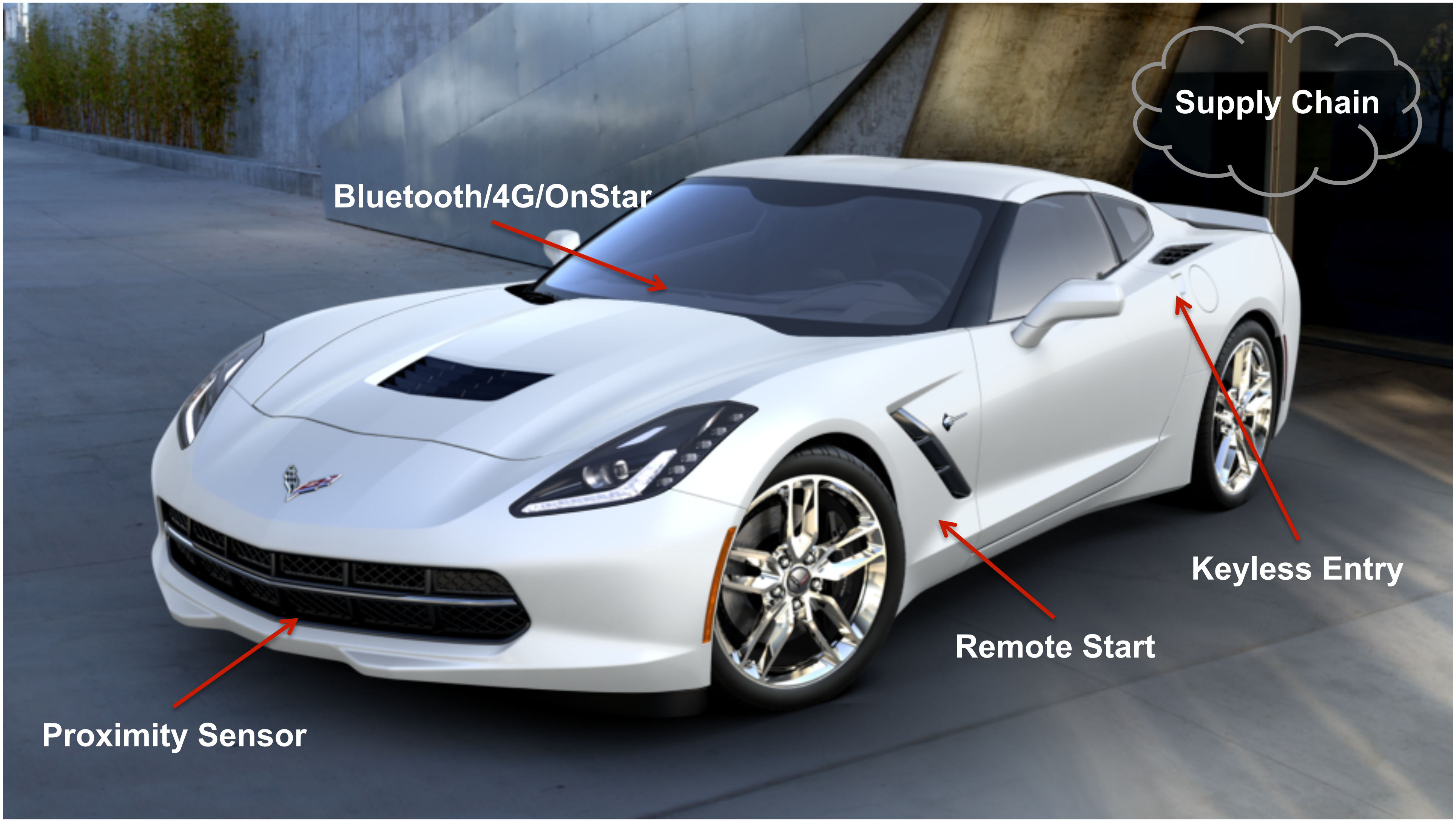


192.168.0.63

...and I just hacked a bank.

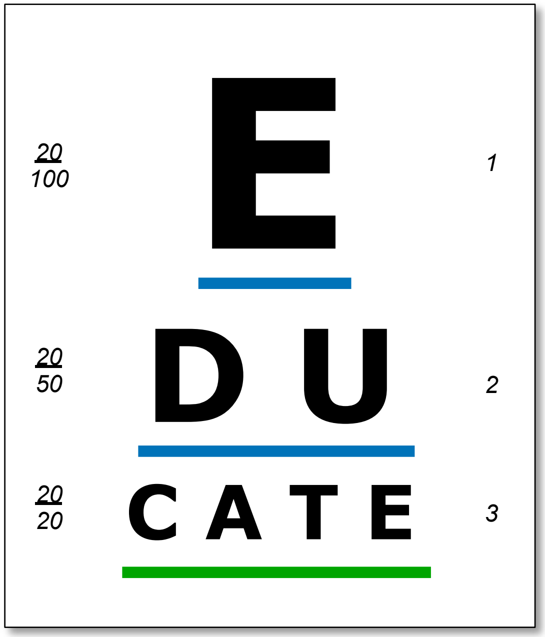
Cyber Threats…Are They Really Everywhere?

NORTHROP GRUMMAN

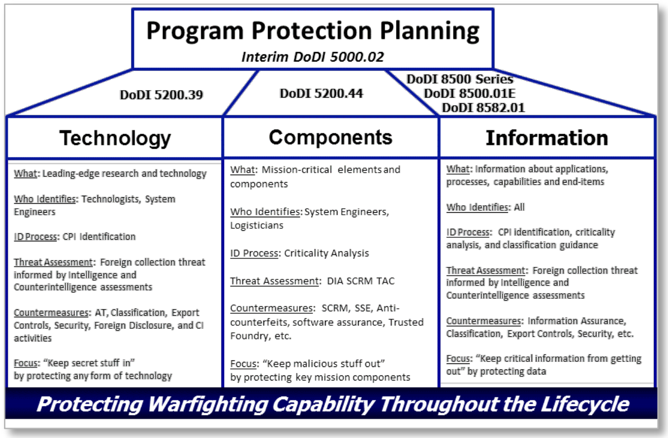


Secure Engineering and Vulnerability Analysis Greatly Reduces the Risk of Cyber and Supply Chain Attacks

Maintain your Vision with Education



- We have several classes in our internal Cyber Academy to account for topics such as Secure Architecture and Secure Coding
- We conduct internal symposiums at various locations around the country
- We educate our application developers about risks to the supply chain and what to watch for
- We use training material from customers to stress importance of material to the audience

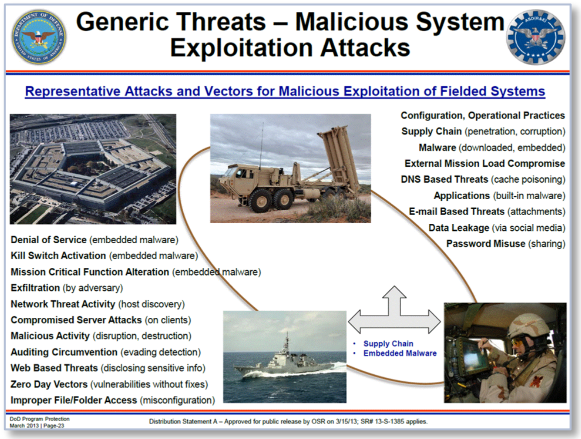


Program Protection Planning

Interim DoDI 5000.02

DoDI 5200.39	DoDI 5200.44	DoDI 8500 Series DoDI 8500.01E DoDI 8582.01
Technology	**Components**	**Information**
What: Leading-edge research and technology	What: Mission-critical elements and components	What: Information about applications, processes, capabilities and end-items
Who Identifies: Technologists, System Engineers	Who Identifies: System Engineers, Logisticians	Who Identifies: All
ID Process: CPI Identification	ID Process: Criticality Analysis	ID Process: CPI identification, criticality analysis, and classification guidance
Threat Assessment: Foreign collection threat informed by Intelligence and Counterintelligence assessments	Threat Assessment: DIA SCRM TAC	Threat Assessment: Foreign collection threat informed by Intelligence and Counterintelligence assessments
Countermeasures: AT, Classification, Export Controls, Security, Foreign Disclosure, and CI activities	Countermeasures: SCRM, SSE, Anti-counterfeits, software assurance, Trusted Foundry, etc.	Countermeasures: Information Assurance, Classification, Export Controls, Security, etc.
Focus: "Keep secret stuff in" by protecting any form of technology	Focus: "Keep malicious stuff out" by protecting key mission components	Focus: "Keep critical information from getting out" by protecting data

Protecting Warfighting Capability Throughout the Lifecycle



Generic Threats – Malicious System Exploitation Attacks

Representative Attacks and Vectors for Malicious Exploitation of Fielded Systems

Configuration, Operational Practices
Supply Chain (penetration, corruption)
Malware (downloaded, embedded)
External Mission Load Compromise
DNS Based Threats (cache poisoning)
Applications (built-in malware)
E-mail Based Threats (attachments)
Data Leakage (via social media)
Password Misuse (sharing)

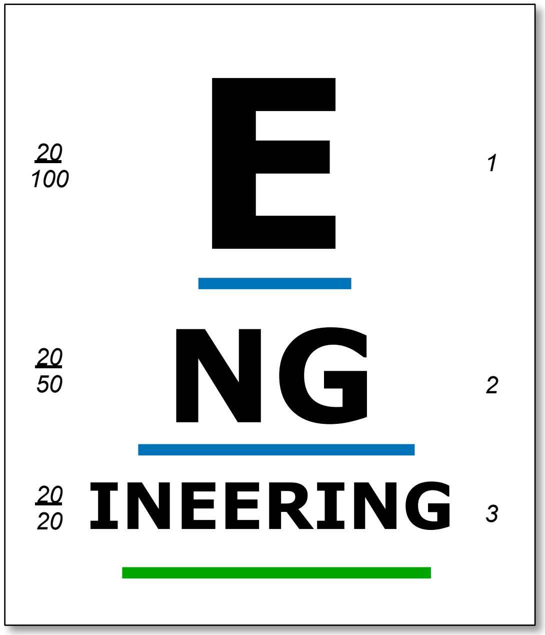
Denial of Service (embedded malware)
Kill Switch Activation (embedded malware)
Mission Critical Function Alteration (embedded malware)
Exfiltration (by adversary)
Network Threat Activity (host discovery)
Compromised Server Attacks (on clients)
Malicious Activity (disruption, destruction)
Auditing Circumvention (evading detection)
Web Based Threats (disclosing sensitive info)
Zero Day Vectors (vulnerabilities without fixes)
Improper File/Folder Access (misconfiguration)

- Supply Chain
- Embedded Malware

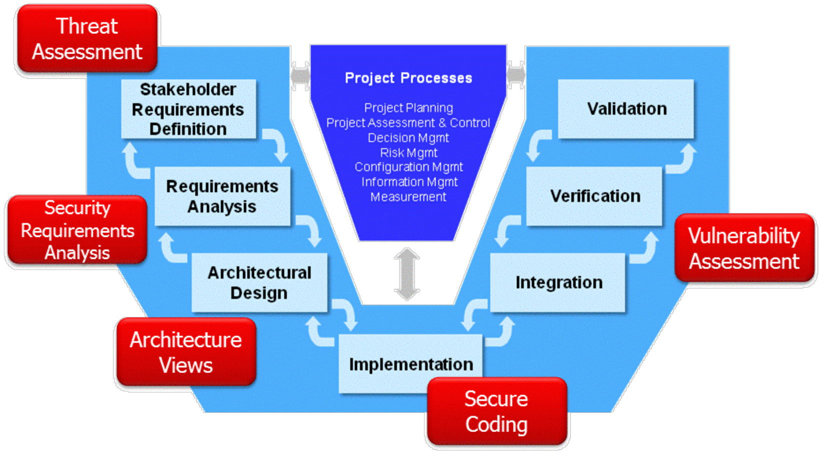
DoD Program Protection
March 2013 | Page-23

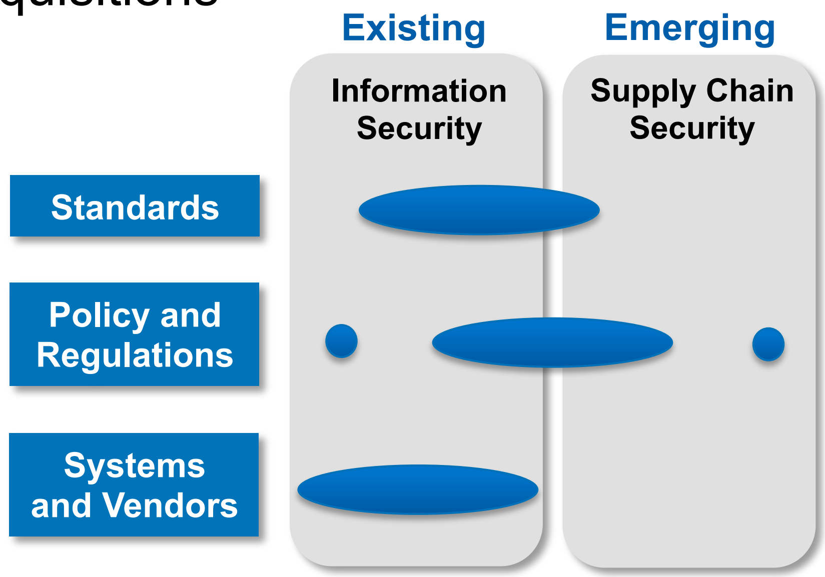
Distribution Statement A – Approved for public release by OSR on 3/15/13; SR# 13-S-1385 applies.

Focus on Engineering

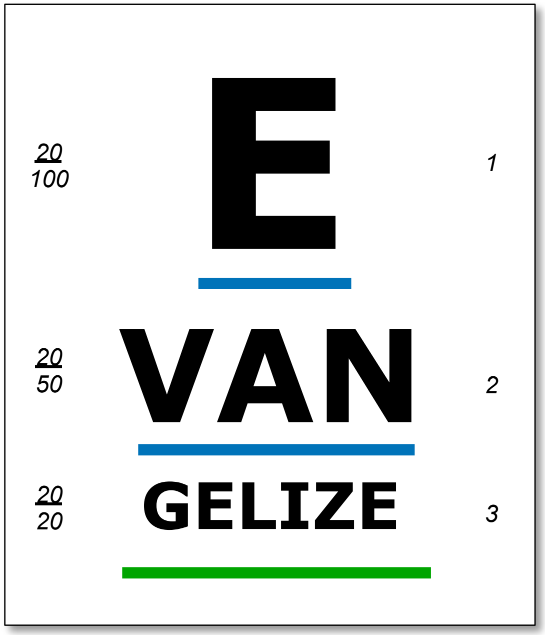


- The development of processes around System Security Engineering is a natural extension of the formal Systems Engineering process
- Engineering a solid system to protect the integrity of the supply chain is necessary
- New CDRLs, such as security plans and security architecture views, may be required for future acquisitions





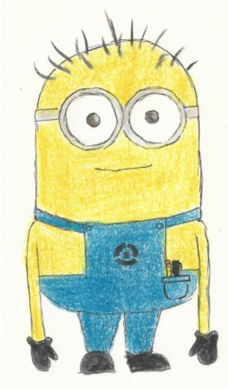
Evangelists Lead Culture Change



- Changing the culture of decades of Systems Engineering is hard work, and requires dedicated evangelists

- Convincing engineers that spending time and money building more secure systems, instead of making the aircraft fly further, is an uphill battle
  - *Especially when their customers haven't expressed an interest in security*

- Grow your own minions!



Original Fan Art by Sierra Papay
Used with permission

Awareness and Recommendations

- Understand that entertainment is raising awareness of threat vectors
  - Popular television shows, such as 24
  - Best selling games, such as **Watch Dogs** *Hacking is my Weapon*
- Look for the unexpected attacks: watering holes, denial of service, etc.
- Ensure that your supply chain is not the weak point in your defense
- Secure the design data of your network – it is critical

THE VALUE OF PERFORMANCE.

NORTHROP GRUMMAN