

T&E Meets APT: A Secure Engineering Perspective from Industry

THE VALUE OF PERFORMANCE.
NORTHROP GRUMMAN

2015 ITEA Cybersecurity Workshop

24 February 2015

Michael Papay, PhD

Vice President

Chief Information Security Officer

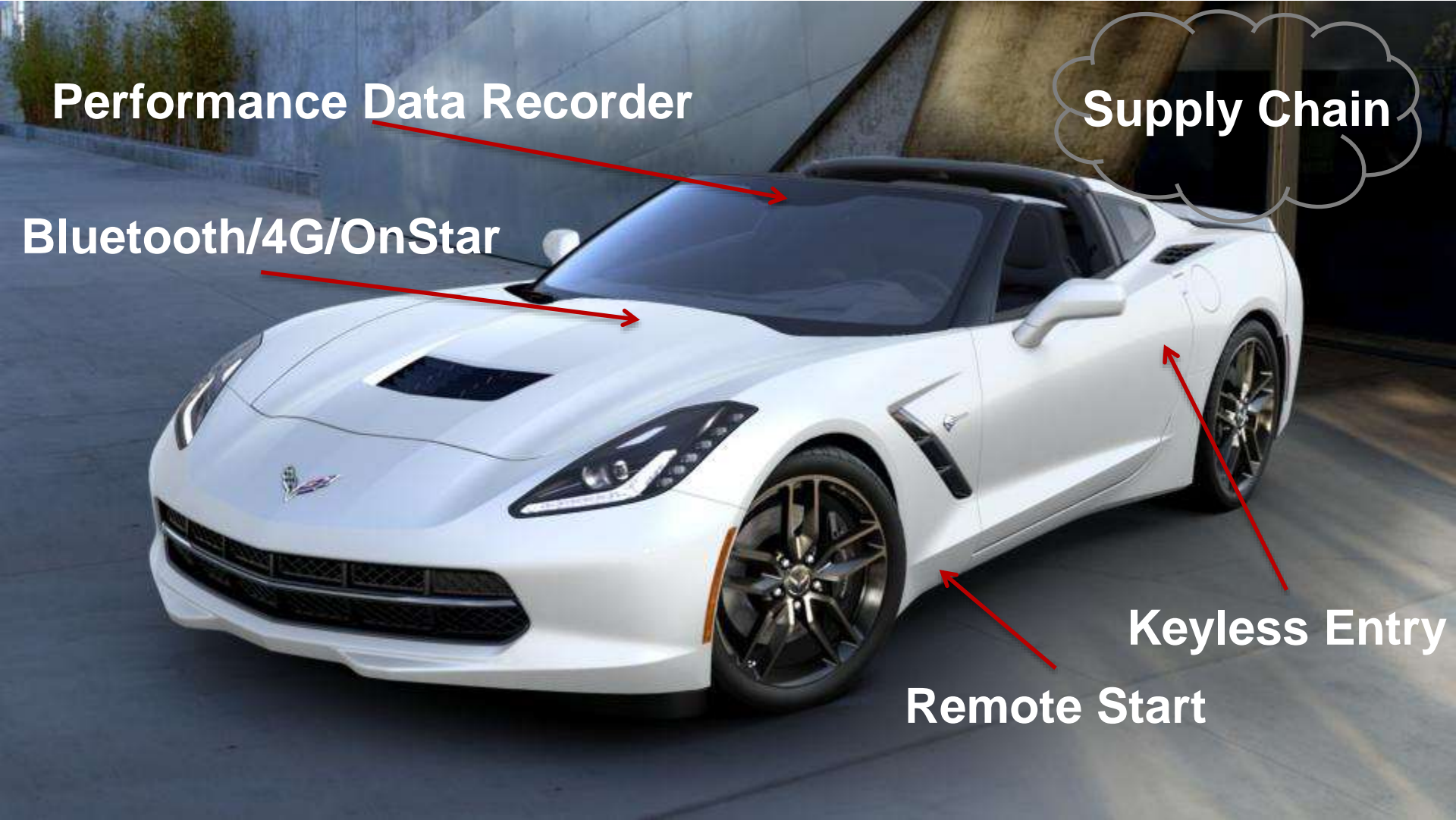
Northrop Grumman

Security Engineering: Simplified

- Continuously improve your C4ISR architecture with security in mind
 - Think: “Secure by Design”
- The Internet of Things (and a lesson for us)



Cyber Threats...Are They Really Everywhere?



Performance Data Recorder

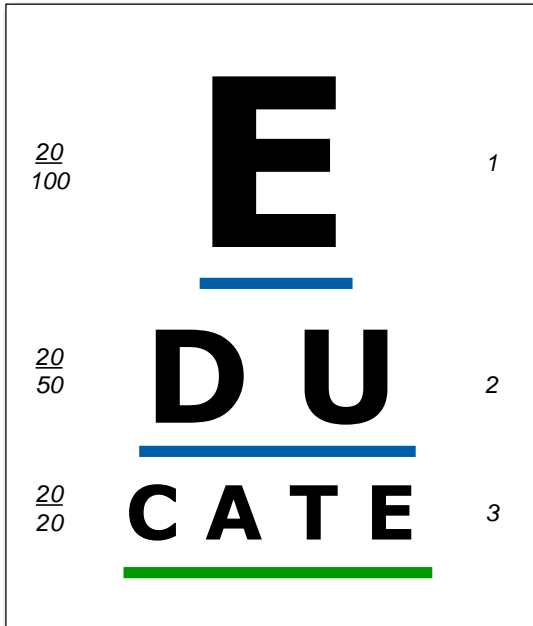
Supply Chain

Bluetooth/4G/OnStar

Keyless Entry

Remote Start

**Security Engineering and Vulnerability Analysis
Enable Successful Cyber Testing**

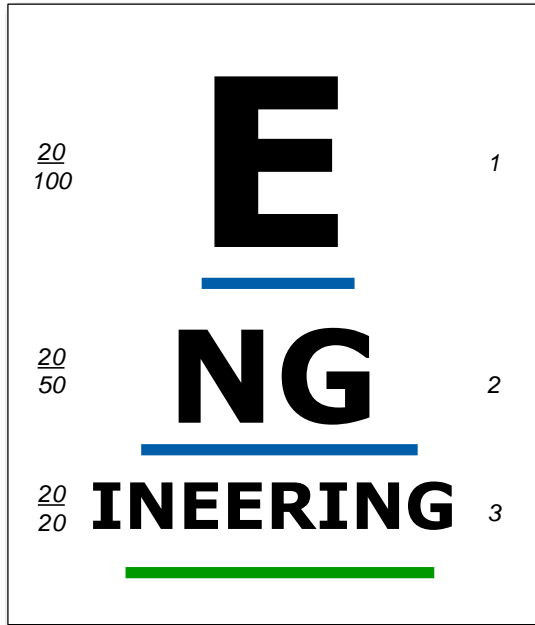


- Industry is starting to account for topics such as Secure Architecture and Secure Coding in their training material
- We educate our application developers about risks to the supply chain and what to watch for
- We use training material from customers to stress importance of material to the audience

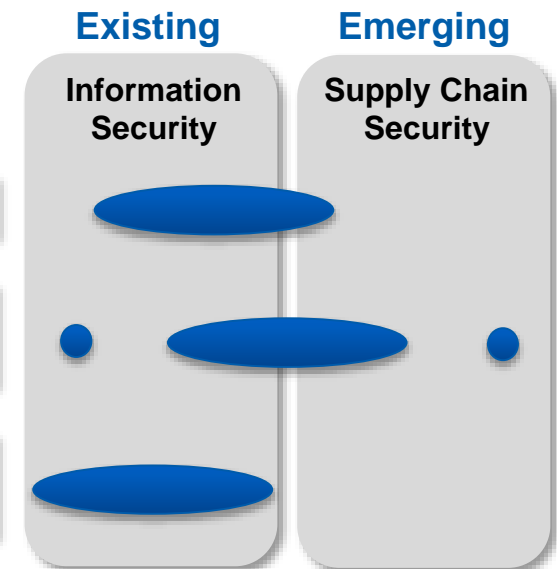
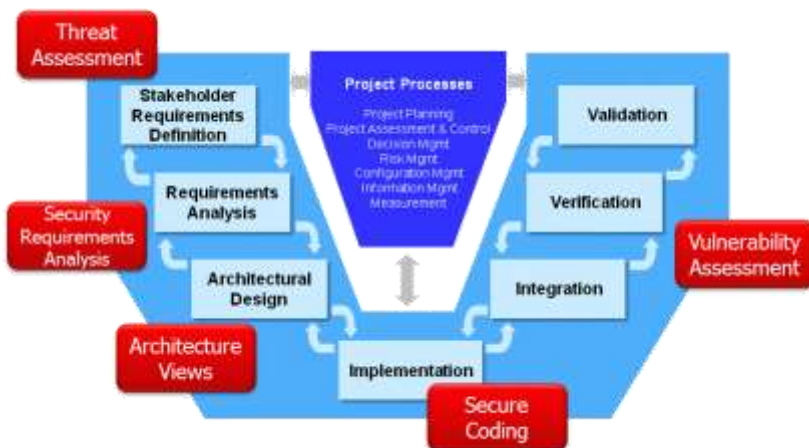
Program Protection Planning Interim DoDI 5000.02		
DoDI 5200.39	DoDI 5200.44	DoDI 8500 Series DoDI 8500.01E DoDI 8582.01
Technology	Components	Information
<p>What: Leading-edge research and technology</p> <p>Who Identifies: Technologists, System Engineers</p> <p>How/Process: CP Identification</p> <p>Threat Assessment: Foreign collection threat informed by intelligence and counterintelligence assessments</p> <p>Countermeasures: AT, Classification, Export Controls, Security, Foreign Disclosure, and C activities</p> <p>Goal: "Keep secret stuff in" by protecting any form of technology</p>	<p>What: Mission-critical elements and components</p> <p>Who Identifies: System Engineers, Linguists</p> <p>How/Process: Criticality Analysis</p> <p>Threat Assessment: DIA SORM 74C</p> <p>Countermeasures: SCRM, SIC, anti-counterfeits, software assurance, Trusted Foundry, etc.</p> <p>Goal: "Keep malicious stuff out" by protecting key mission components</p>	<p>What: Information about applications, processes, capabilities and end-items</p> <p>Who Identifies: AI</p> <p>How/Process: CP Identification, criticality analysis, and classification guidance</p> <p>Threat Assessment: Foreign collection threat informed by intelligence and counterintelligence assessments</p> <p>Countermeasures: Information Assurance, Classification, Export Controls, Security, etc.</p> <p>Goal: "Keep critical information from getting out" by protecting data</p>
Protecting Warfighting Capability Throughout the Lifecycle		



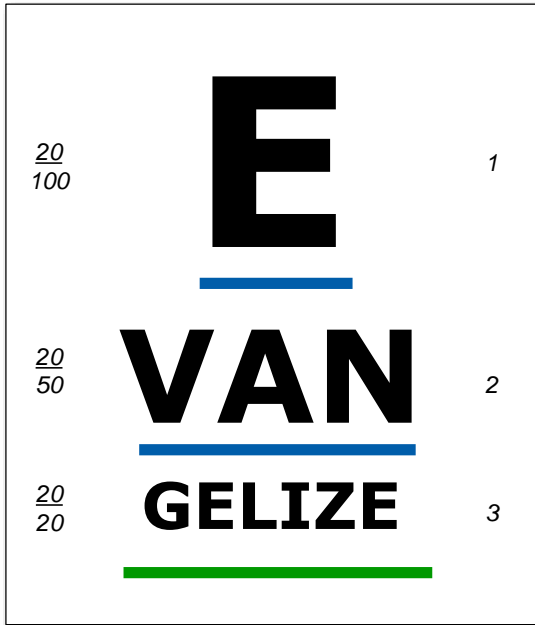
Focus on Engineering



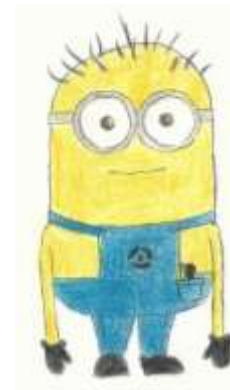
- The development of processes around System Security Engineering is a natural extension of the formal Systems Engineering process
- Engineering a solid system to protect the integrity of the supply chain is necessary
- New CDRs, such as security plans and security architecture views, will be required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



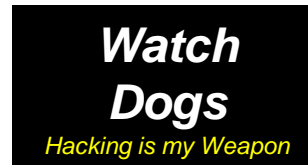
Original Fan Art by Sierra Papay
Used with permission

- Understand that entertainment is raising awareness of threat vectors

- Popular television shows, such as



- Best selling games, such as



- Tighten up the relationship between end users, acquisition teams, and industry to make sure expectations are met
- Ensure that your supply chain is not the weak point in your defense
- Secure the design data of your system – it is critical

THE VALUE OF PERFORMANCE.

NORTHROP GRUMMAN

