Morning Keynote - Greg Shannon

Table of Contents

The overall classification of this briefing is UNCLASSIFIED

NDIA Hard Problems Workshop - Cyber COI Deep Dive

5 Nov 14

Dr. Richard Linderman
Cyber COI Steering Group Lead

This briefing is Approved for Public Distribution. OSD Release #14-S-2118

Distribution A – For Public Release

**001 Shane McGraw: And hello from the campus of Carnegie Mellon University in Pittsburgh, Pennsylvania. We welcome you to the SEI virtual event, CERT Alignment with the Cyber COI Challenges and Gaps. Depending on your location, we wish you a good morning, a good afternoon, or good evening. My name is Shane McGraw. I will be your moderator, and I'd like to thank you for attending. We have a great lineup of cybersecurity experts to speak all day long, and we want to make today as interactive as possible, so we will address questions at the end of each 45-minute presentation. You can submit questions to our event staff at any time during the presentation by using the Questions tab on your control panel.

We will also ask a few polling questions throughout the presentations. They will appear as popup windows on your screen. In fact, the first polling question we'd like to ask is: How did you hear of today's event? Another three tabs I'd like to point out are the Files, Twitter, and Survey tabs. The Files tab has a PDF copy of the slides from each 45-minute presentation today, along with other security-related resources from CERT and the SEI. For those of you using Twitter, be sure to follow @seinews, and use the hashtag #certcyber. Once again, follow @seinews, and hashtag for today is #certcyber.

And now I'd like to introduce our morning keynote speaker for today. Dr. Greg Shannon is the chief scientist for the CERT division at Carnegie Mellon University's Software Engineering Institute, and Shannon is also the chair of IEEE's cybersecurity initiative. And now I'd like to turn the presentation over to Dr. Greg Shannon. Greg, welcome. All yours.

Greg Shannon: Great. Thank you, Shane. It's a delight to be here this morning on the third day of summer. It's nice and cool inside. I hope you all are also enjoying a climate-controlled environment as you view either this webinar live or recorded.

The goal of today's webinar is to really try and connect the researchers, the staff at CERT, into the broader issues of the Department of Defense Communities of Interest.

That's what COI stands for, the Communities of Interest. This is part of a broader effort within the DoD called Reliance 21, and it's to blend in-- or to align the R&D efforts of the broad DoD enterprise. The broad DoD enterprise has 35 thousand scientists and engineers at 62 DoD labs, and then you add to that the 10 thousand engineers and scientists and staff at ten DoD FFRDCs. So it's quite a large enterprise, and the goal of Reliance 21 is to bring that all together as a national capability to provide national security for this country.

So what's the role of the CERT division in this endeavor? We're part of an FFRDC, the Software Engineering Institute, operated by Carnegie Mellon University. The CERT division has been around for 25 years. SEI has been around for 30-plus years. We've been involved in cybersecurity-- many people often confuse us with the Department of Homeland Security's US-CERT. We have a long legacy with them and a strong connection with them, but fundamentally we are a Department of Defense laboratory, and that's part of the goal of today's webinar is to bring that together and to help make it clear how that connects in with the R&D priorities of the Department of Defense by giving you specific examples of what we're up to.

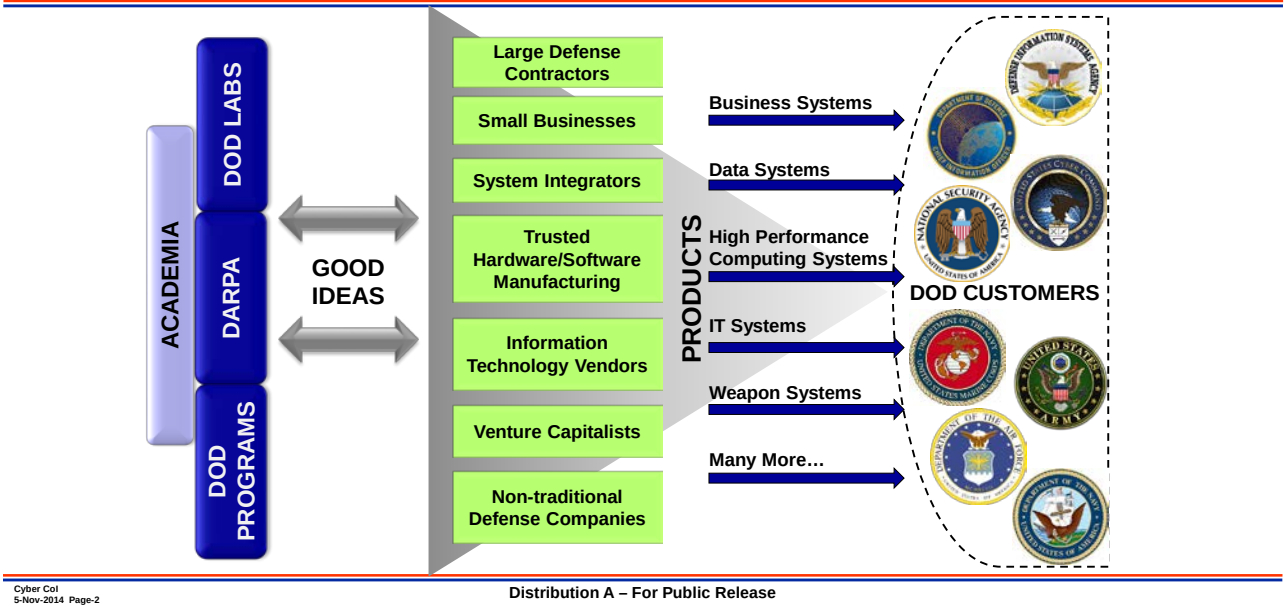
Part of what makes an FFRDC a special capability for the nation is the fact that it brings together a government perspective, and industry

perspective, and an academic perspective simultaneously, and that's what an FFRDC, a research FFRDC in particular, sits at the nexus of. So hopefully what you'll learn today as part of our presentations and technical material that we present is to understand how that looks different than what you might hear from industry or academia, or specifically from the government, and how we bring that together.

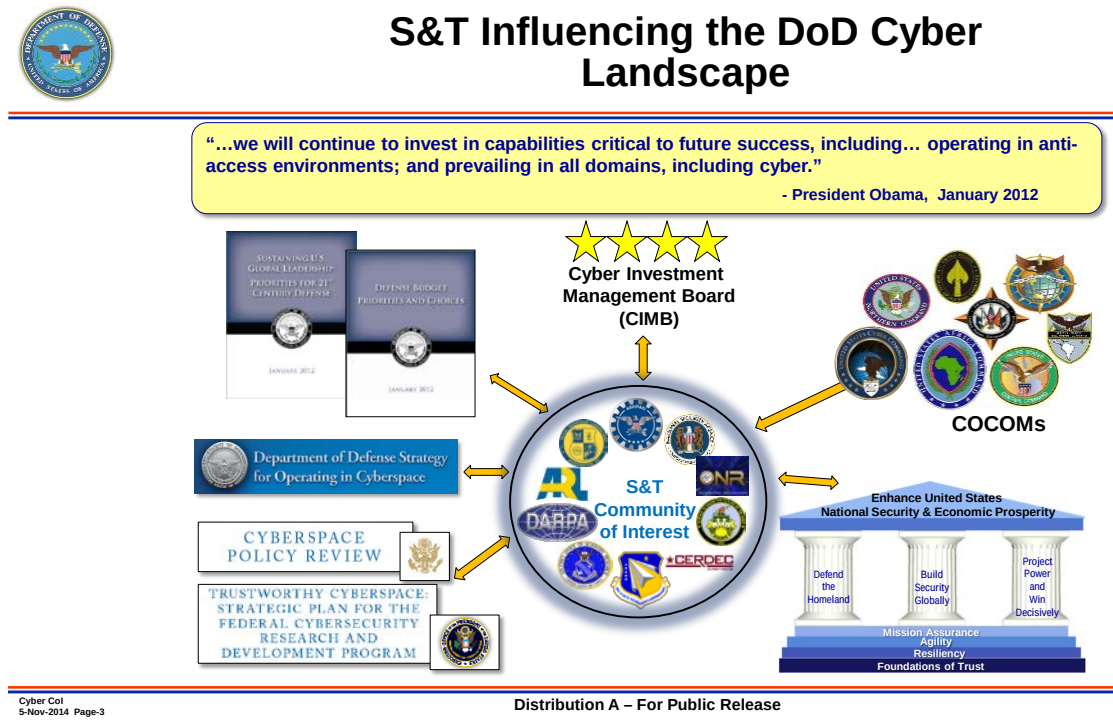
So I'm delighted to have the specific technical talks that we have today, as well as the panels that can have a conversation about how to pull that together. I really do encourage you to ask us questions that can challenge us and give you as much information as possible.

So with that, I want to do a walkthrough of what the Cyber Community of Interest is. There's 17 other communities of interest as part of Reliance 21. These are slides that-- so I'm going to use slides now that Dr. Rich Linderman, who's the group lead for the Cyber COI, gave back in November as part of an NDIA conference. So these are not my slides, but the goal in using these particular slides is to show that we are focused on the DoD S&T challenges-- science and technology challenges-- and this really is the framework, the context, for the webinar today.

DoD Cyber Ecosystem

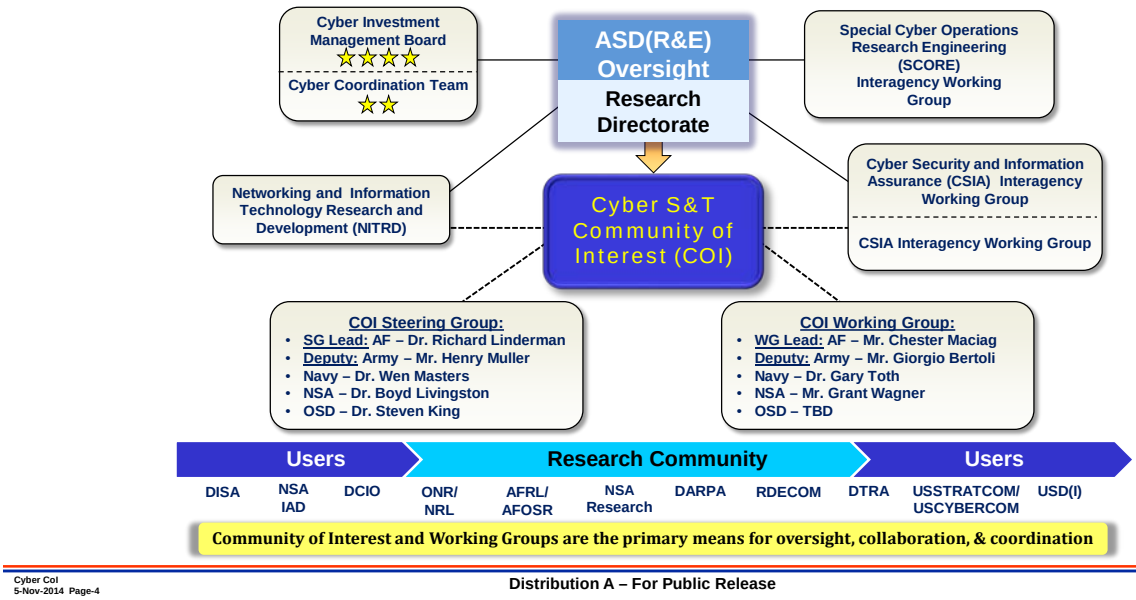


**002 This is the way that the Department of Defense looks at the ecosystem in general. I mean, this one is particular for Cyber, but you really could put any of the other COIs as part of this ecosystem, and it shows how there's this pipeline of ideas that are trying to get from academia, from DARPA, the DoD labs-- it goes through people who really make it happen to produce products and capabilities for national defense, and finally ends up as capabilities for our customers, our DoD customers-- the Army, the Navy, the Air Force, the Marines, and the-- what's the fifth one? Coast Guard. Thank you. Sorry. So that's the ecosystem that we work in and are part of.



**003 The Cyber COI has been going on for a while and pulls in many-- it's driven by policy broadly within the government. By the way, these slides are also available online, the full set. I've taken a subset of the original presentation that Dr. Linderman gave to kind of focus more on the technical elements, but do want to give you a sense of how, again, this all fits together.

DoD Cyber S&T Coordination

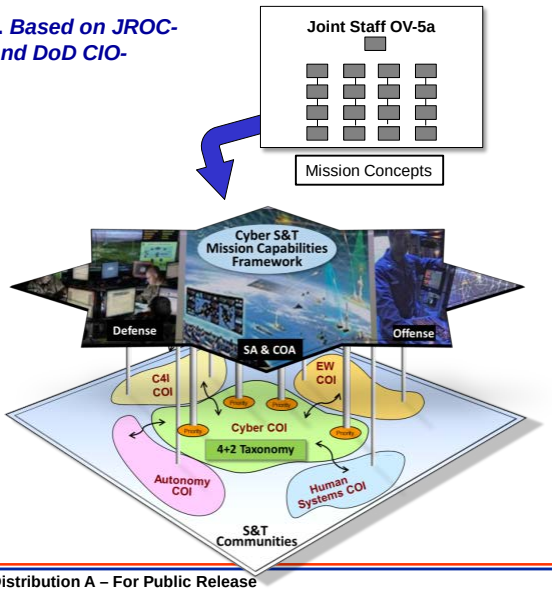


**004 Again, there's plenty of coordination to keep various people aligned.

Cyber COI - Scope

An Operational Domain: JS OV-5a. ***Based on JROC-Approved Capability Documents and DoD CIO-developed Architectures***

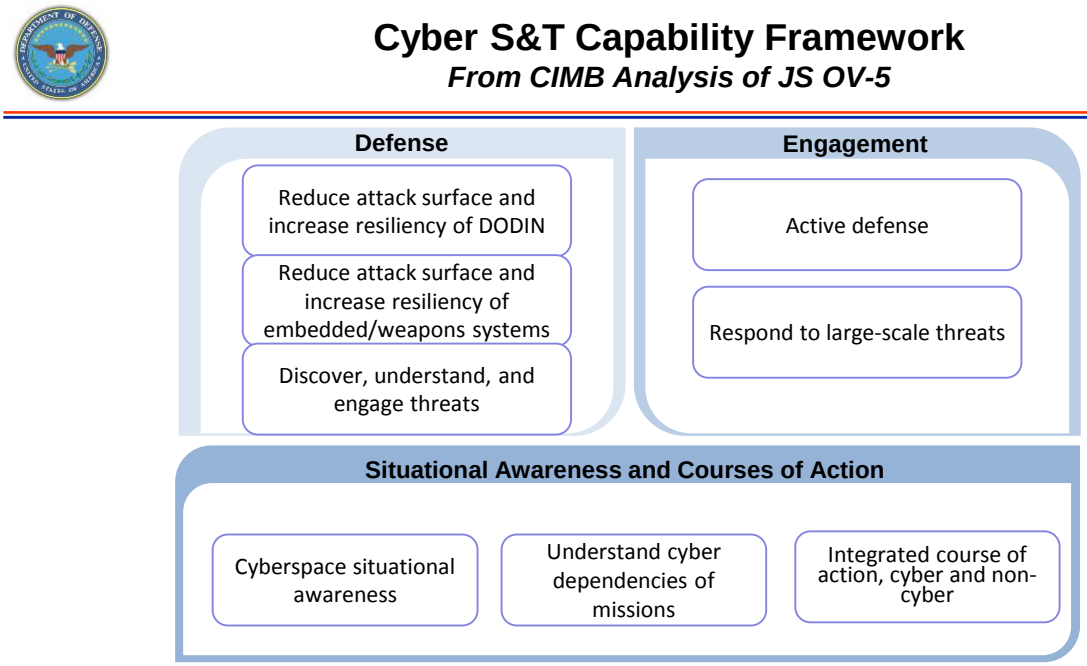
- Spans Defense, Effects, Situational Awareness-Course of Action
- Includes enterprise, tactical and embedded
- Cuts across all domains
- Touches C4I, EW, Autonomy, and Human Systems COIs
- Transcends S&T across all DOTMLPF
- QDR Tenets Addressed
  - Mitigates Threats
  - Delivers Affordable Capability
  - Affords Technological Surprise



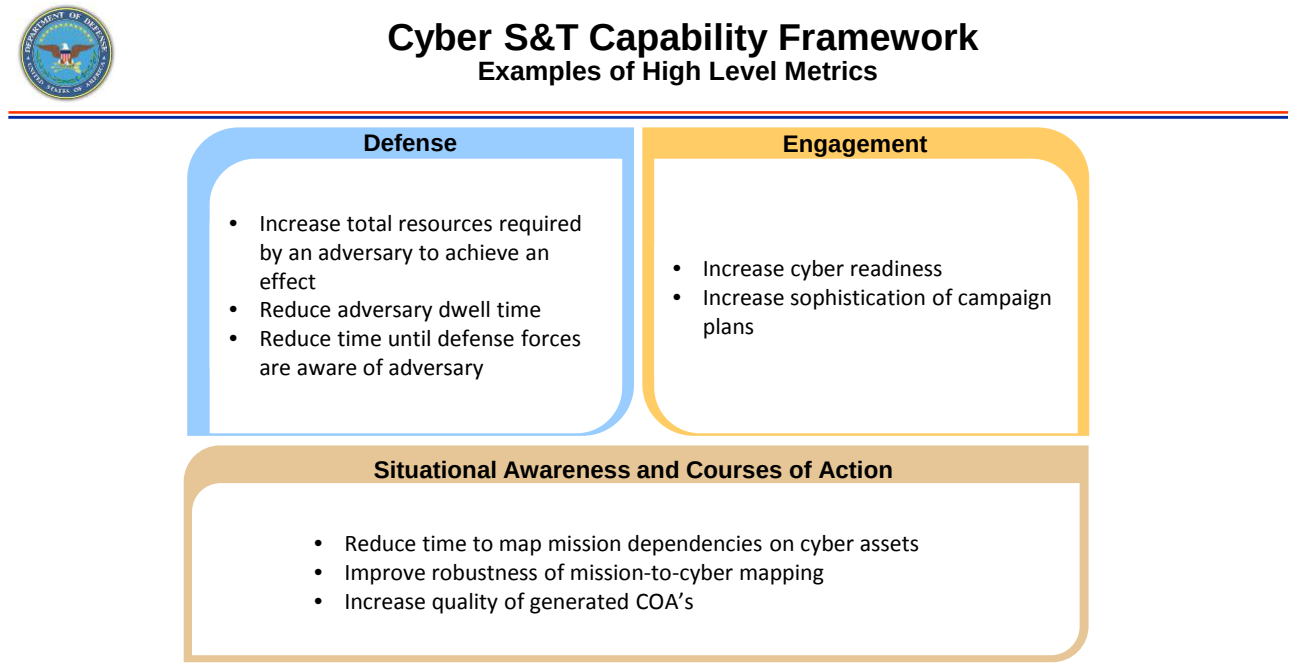
Distribution A – For Public Release

**005 The scope here is that it's really-- defense affects capabilities that we deliver and it cuts across all domains. There are related COIs such as C4IEW, which is Electronic Warfare, Autonomy, Human Systems. This is fed by demands that the COCOMs and people in the field have for technology, and usually people in the field don't necessarily have a strong sense of, well, what's the particular technical capability they need? They talk about a mission capability. And so part of the goal of the COIs as well as the broader Reliance 21 is to take needs of the customers, of those in the field, and interpret them in terms of what are the science and technology needs that we need to drive forward in order to provide national capabilities.

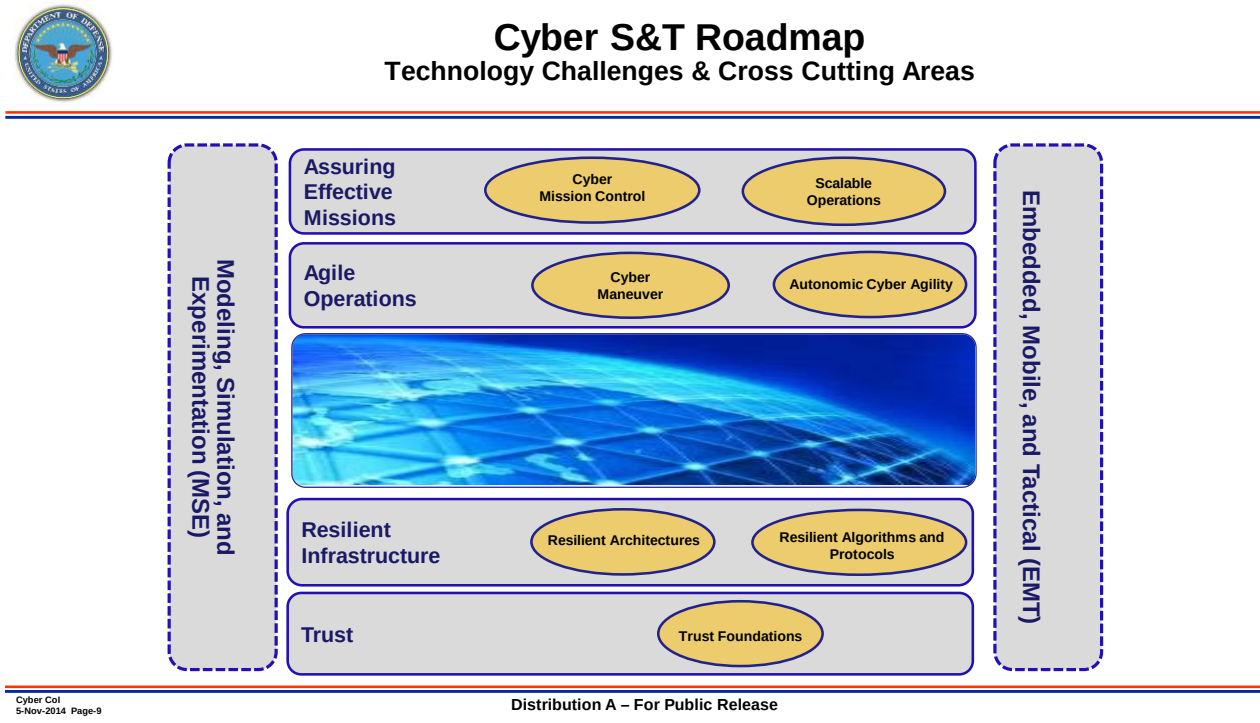
Cyber S&T Capability Framework
From CIMB Analysis of JS OV-5



**007 In terms of what the capabilities are that have been identified that really need to be broadly addressed cover kind of three areas: defense, engagement, situational course of action. These are not necessarily technical areas, they're just technical aspects, but these are really the capabilities that the Department of Defense is trying to get to, and part of the challenge here is how do you measure the nation's ability, the Department of Defense's ability to provide these capabilities operationally as well as from a technology point of view.



**008 And important part of this is looking at metrics. This is actually work that we've been involved here, and we won't hear about today, but it's really part of a key aspect, and as you hear these presentations you'll have a strong sense that there is a notion of effectiveness and measurement as part of how researchers at CERT think about these problems, and that's a key driving challenge broadly within the Cyber COI.



**009 The roadmap that the Cyber COI uses as its touchstone-- so this is where the capabilities are now interpreted in terms of what are the S&T needs for Cyber.

So there's four primary areas, and I'm either delighted to say or apologize that I was actually involved in helping form this. This roadmap was formed about four years ago as part of collaboration within the ecosystem that I showed earlier of national defense labs, national labs, users from the field to pull it together to identify what are the key technical challenges. So what I'll do is I'll spend a little bit of time on each of these areas to talk about what those challenges are, but these really are driven by what are the nation's

current needs, because you could-- nation's current defense needs-- because you could broaden this and you could say there are other security challenges out there that maybe need to be addressed. But these really are framed in terms of national defense needs. So assuring-- let's see, let me go to the next slide here.

DoD's Joint Cyber S&T Focus Areas

DoD's Joint Cyber S&T Focus Areas

Assuring Effective Missions	Assess & control the cyber situation in mission context
Agile Operations	Escape harm by dynamically reshaping cyber systems as conditions/goals change
Resilient Infrastructure	Withstand cyber attacks, while sustaining or recovering critical functions
Trust	Establish known degree of assurance that devices, networks, and cyber-dependent functions perform as expected, despite attack or error
Embedded, Mobile, & Tactical (EMT)	Increase the capability of cyber systems that rely on technologies beyond wired networking and standard computing platforms
Modeling, Simulation, & Experimentation (MSE)	Simulate the cyber environment in which the DoD operates to enable mission rehearsal and a more robust assessment and validation of cyber technology development

CROSS CUTTING

Distribution A – For Public Release

**010 So assuring effective missions is, in the mission context, does a commander have assurance and have a sense of likelihood that the capability is available that he wants and that it'll be successful in a mission setting?

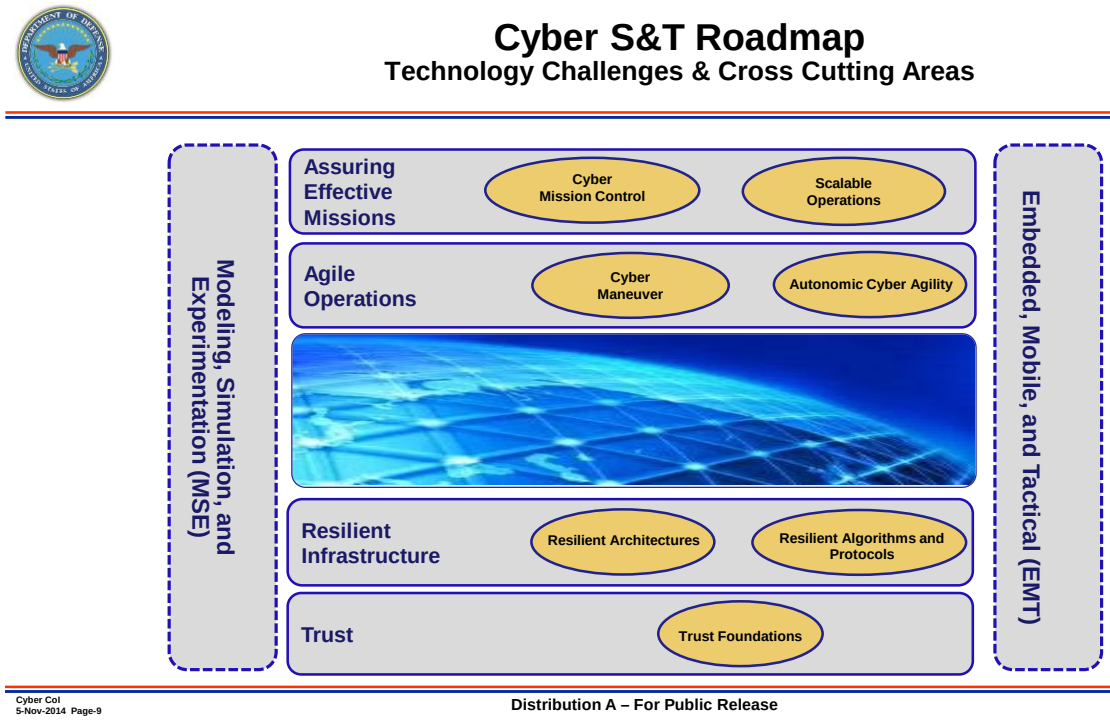
Agile operations means to be able to escape from harm dynamically, and that dynamic element is really

important, and actually very difficult. Many IT systems are configured and they're fairly static, which makes an easy target. If an adversary is attacking a system, you want to be able to maneuver and adapt quickly. You'll hear actually a very nice panel at the end of the day on DevOps, which is, in our view, part of the mechanism to have an agile response to threats, where you have to actually develop new capabilities very quickly.

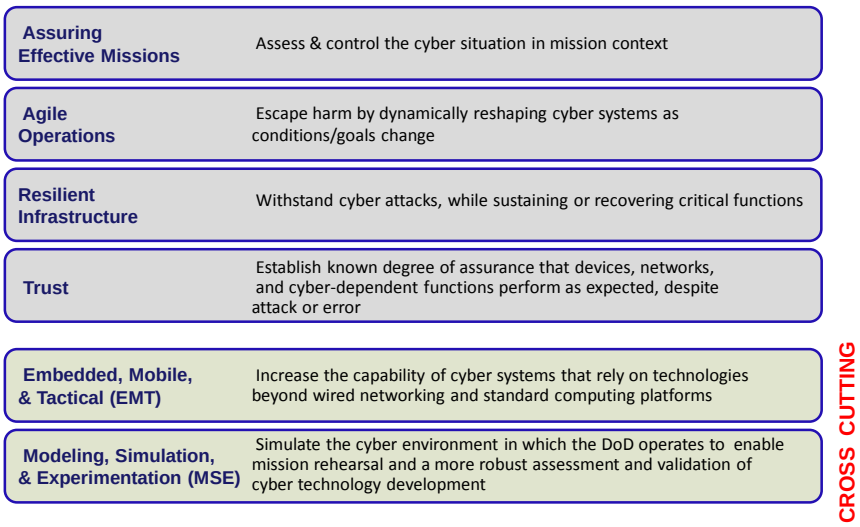
Resilient infrastructure means you're able to withstand attacks. So I think in terms of a boxer. A boxer has to be agile, has to be able to dodge the punch coming at him, but he also has to be resilient, because sometimes the punch is going to land on you and you can't crumble under attack, and you need to carry on. This ties in with another panel that we'll have on resiliency. This is a long-standing body of work that we have that looks broadly at the problem of challenge, and it actually emphasizes the unique capabilities that CERT brings to the table in terms of looking broadly beyond just DoD to learn lessons from the commercial sector, from the financial services sector, and bring that into a broader perspective on resilient infrastructure; because it's very easy from a Department of Defense point of view to focus on, say, the forward operations challenges, the war fighter who's in harm's way, but it's becoming more and more apparent that a key component of cybersecurity is protecting the logistics side, the

operations side, those in the back office that are making sure that the supplies are there on time that do the logistics planning, the mission planning. That's a key component of our effectiveness also. And so being able to provide resiliency, both from a military systems, weapons systems point of view, as well as from a backend logistics, IT infrastructure, that we're only becoming more and more reliant on. Trust then is really considered the foundation.

Cyber S&T Roadmap
Technology Challenges & Cross Cutting Areas



**009 In the previous notion, you have trust there down at the bottom, trust foundations.



**010 Trust really is a key component for providing national capability in Cyber. So it provides a known degree of assurance. And it's not a matter of total assurance, usually, because that's actually very expensive to achieve, but what's the degree of known assurance that the networks, devices and cyber-dependent functions will perform as expected in spite of attack, in spite of an error? And that really ties back then again to the metrics challenges that we're working with the DoD to address and to be more specific about. But trust really is a foundation. You'll see that we've got a number of talks this morning also. When I get done here, I'll actually step through the presentations and talk about which talks are affiliated with which focus area.

The two cross-cutting areas are embedded mobile and tactical, and that's relevant particularly for the warfighter in harm's way, those who are in the field having to deal with the technical challenges of equipment that is directly under fire, if you will, whether it's kinetic fire or cyber fire, and we want to increase the capability of that. A big part of that is being able to tie, again, back into commercial infrastructure-- not the commercial infrastructure-- commercial products that warfighters are often used to using in civilian life. How do you bring those capabilities into the tactical and embedded environment, because you clearly can't bring your own device to work in those situations, but what devices can you have access to and how can we bring those similar sorts of capabilities that people are used to in their everyday life and take advantage of?

The modeling simulation and experimentation component is really about how do you do better science and engineering. What are the tools you need for better science and engineering in the cyber arena? Clearly cyberspace is very complex. It's difficult for one to get a clear understanding of it. I've talked to people within the DoD about how adversaries are often better scientists in terms of understanding infrastructure and how to attack it than we are sometimes, and the reason is they have so little information, the only way they can attack this is to actually understand what's really there.

But as defenders, we have the advantage that we can change that environment, and we can explore possibilities. So part of modeling and simulation is to understand really what are the possibilities of how to defensively respond, how to anticipate adversary actions and mitigate those, how to evaluate different technologies for efficacy.

Measurement is an important part of that experimentation component. You want to be able to measure-- have some sense of success and failure in a quantitative manner for the broad areas of cyber.

Specific Gap Assessment

Specific Gap Assessment

Defense

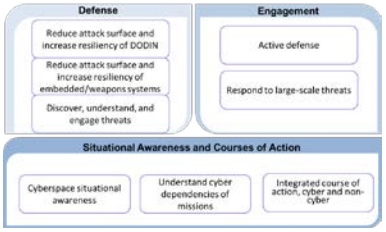
- **Trustworthy embedded system architectures composed of components of mixed trust**
- **Trust scoring mechanisms**
- **Scalable HW/SW analysis and verification techniques**
- **Resilient mobility**

Engagement

- **Control planes for heterogeneous components and systems**
- **Threat-aware defenses**
- **Real-time defensive traffic management**

Situational Awareness and Courses of Action

- **Graded options responsive to commander's intent**
- **Analysis of Mission Dependencies to Cyber Infrastructure**
- **Cyber-Kinetic integration, planning, and assessment**



Measurement and Metrics

- **Quantifiable attack surface measurement**
- **Component and system resiliency metrics**
- **Threat-based agility metrics**
- **Calculus for Mission Assurance**
- **Cyber modeling and simulation and experimentation**

Cyber CoI
5-Nov-2014 Page-11

Distribution A – For Public Release

**011 So I'm going to go through these six areas again in terms of kind of the general roadmaps, but really

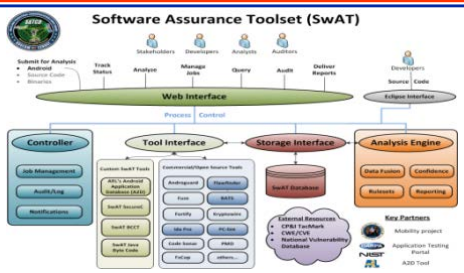
one of the key outputs of the roadmap is what are the gaps, what are the technical gaps, and what I hope you see today is how much of the research that we're doing aligns very directly with these gaps, in terms of these are the challenges where more effort is needed, where more inspiration is needed. So on the notion of trustworthy embedded system, resilient mobility, threat-aware defenses, you'll see those elements in the talks today, and this in some sense is kind of the key problems that we focus on at CERT in terms of trying to frame out our research plan. Excuse me while I cough. Thank you.

So let's move on to some of the specifics here.

Trust Foundations
Objectives / Accomplishments / Challenges

Objectives:

- **Trusted Components and Architectures**: Develop measures of trustworthiness for cyber components and large systems of varying pedigree and trustworthiness
- **Scalable Supply Chain Analysis and Reverse Engineering**: Analyze, attribute, and repurpose hardware and software at the speed and scale required for real-time strategic engagement



Accomplishments:

- FY13/14 Success Stories
  - Army: SW Assurance Toolkit (SWAT)
  - AF: Secure Processor
  - AF: Context/Content Aware Trusted Router
  - AF: Secure View

Technical Challenges:

- Development of Trust Anchors for component-level and composed HW and SW
- Tamper-proof/evident HW and SW components and systems
- Contextual threat/trust scoring calculus
- Rapid, assisted, and automated HW and SW analysis and validation
- Algorithms for accurate attribution of malware authors and supply chain tampering

Distribution A – For Public Release

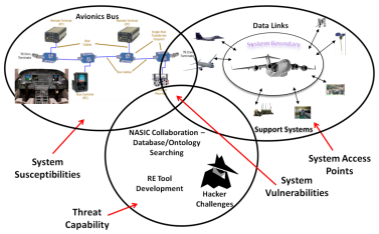
**012 So in terms of trust foundations, trusted components, trusted architectures is an important aspect. But even the word trust is not necessarily easy to get one's arms around. There's degrees of trust in terms of you have a formal mathematical proof that this capability is going to perform as you expect, to where you have a collection of smart engineers and scientists look at the capability and say, "Yeah, I don't see how an adversary can thwart this capability," or "Here's a way they can thwart it, and here's going to be the mitigations that we have." And there's that full range, and part of the work that we do here is to make that development of trust and estimation and analysis of trust more efficient. Running a full mathematical proof is expensive, so

we look at techniques to improve the efficiency there, and it's algorithms to understand how the adversary is behaving also. How can the adversary affect the trust of our systems is a part of that. So understanding reverse engineering and being able to reverse-engineer threats and such.

Resilient Infrastructure

Resilient Infrastructure
Objectives / Accomplishments / Challenges

Objectives:
- **Resilient Architectures:** Develop integrated architectures that are optimized for the ability to absorb shock and speed recovery to a known secure operable state.
- **Resilient Algorithms and Protocols:** Develop novel protocols and algorithms to increase the repertoire of resiliency mechanisms available to the architecture that are orthogonal to cyber threats.



Accomplishments:
- FY13/14
  - Army DEFIANT
  - Army: CRUSHPROOF

Technical Challenges:
- Assessment environments and tools for measuring resiliency of HW, SW, networks, and systems
- Calculus for relating resiliency concepts into measurable operational impact and automated DODIN defense actions
- Resilient overlay control planes that orchestrate defense of heterogeneous DODIN systems
- Secure, LPI/J, energy-efficient, mobile communication protocols
- Certifiable, agile, and affordable mobile device HW, OS, and app ecosystem

Cyber CoI
5-Nov-2014 Page-13

Distribution A – For Public Release

**013 Resilient infrastructure. Again, as I said before, develop integrated architectures and have a clear sense of how you measure resiliency. Protected the DoDIN, the Defense Information Network, is really the key challenge there. Part of one of the national benefits of these programs is that they will be able to inform the commercial sector about how they can protect their

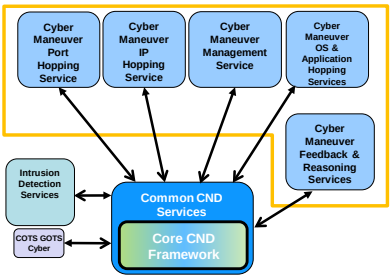
systems more effectively. But it's a two-way street also in terms of incorporating lessons learned from large-scale commercial operations and how they protect themselves and make themselves resilient.

Agile Operations

Agile Operations
Objectives / Accomplishments / Challenges

Objectives:

- **Cyber Maneuver:** Develop mechanisms that enable dynamically changing cyber assets to be marshaled and directed toward an objective – to create or maintain a defensive or offensive advantage
- **Autonomic Cyber Agility:** Speed the ability to reconfigure, heal, optimize, and protect cyber mechanisms via automated sensing and control processes



Accomplishments:

- Army: MorphiNator
- AF: ARCSYNE/COSYNE

Technical Challenges:

- Real-time, mission-aware traffic engineering including routing of threats
- Collaborative, coordinated cyber maneuver of multiple actors and forces (including coalition)
- Cyber maneuver for deceiving threats
- Dynamic reconfiguration of networks, systems and applications
- Autonomous reconfiguration

Cyber CoI
5-Nov-2014 Page-14

Distribution A – For Public Release

**014 The agile operations-- it's interesting how many people we talk to get confused between the difference between agility and resiliency, and again, I go back to the boxer analogy. The agile operations is the ability to duck the punch, to duck the hit, but in order to do that you really have to have a sense of what the situation is, so this is where situational awareness comes in. You need to be aware of your environment, understand what's the important elements in cyberspace

that are affecting how you might move and then being able to effectively move in a timely manner. Timely manner here could be anywhere from days as you prepare for a mission, to milliseconds as you're trying avoid a denial-of-service attack or new malicious malware that the adversary has decided to throw at you.

So that agility element is probably one of the most difficult to implement, but it also then ties into the autonomy COI in terms of the advances in technology they're making there, and how the human is involved in this operation. Because typically a key part of the agile operation is it's part of a decision challenge. You've got an operator, you have a warfighter, you have a commander who's trying to make a decision based on the current situation about how they should adjust their behaviors, how they should adjust their plans, and you want to be able to present useful information, useful decisions to them, and the decisions that they don't need to make, you want to make sure that you make those for them, especially the ones that need to be made within milliseconds.

Assuring Effective Missions

Assuring Effective Missions
Objectives / Accomplishments / Challenges

Objectives:

- **Cyber Mission Control:** Develop tools and techniques that enable efficient models of cyber operational behaviors (cyber and kinetic) to determine the correct course of action in the cyber domain
- **Scalable Operations:** Develop ability to operate and survive during operations conducted by large-scale threats

Accomplishments:

- Promised last year for FY13
  - OSD: Purple Musket
  - Navy: Flying Squirrel BT Integration
- FY13/14 AF: Mission Aware Cyber C2 (MACC2)

Technical Challenges:

- Tools for mapping and real-time analysis of missions to enable cyber/kinetic situational awareness
- Understanding dynamically evolving missions and their dependencies, identifying cyber/kinetic change indicators, updating models and resolving cross-dependencies, projecting change trends
- Decision Support and reasoning tools that factor in multiple dimensions (e.g., attribution, severity, reversibility of effect, BDA, …)

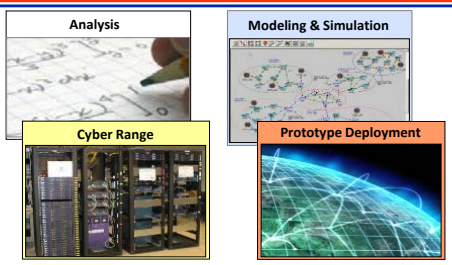
Cyber CoI
5-Nov-2014 Page-15

Distribution A – For Public Release

**015 And then finally, assuring effective missions is really where it comes all together. Part of the message of the Cyber COI is that you want to get to this point, where you have assurance about the mission and the probability of success for different courses of action, but you can't start there. You have to start at the foundations of trust, build up resiliency, build up agility, and then you can have assured effective missions. And that's okay that the warfighters-- it's like, "This is what they want. Why do I need this other stuff?" But clearly as technologists we know this is where we're trying to get to and we need these other components to get there. Let's see. Watch my time here.

Modeling, Simulation, & Experimentation
Objectives / Accomplishments / Challenges

Objectives:
- **Simulation and Experimentation Technology**:
  - Enable robust, quantifiable, and repeatable assessment and validation of candidate cyber technology
- **Models & Analysis:**
  - Simulate the cyber operational environment with high fidelity
  - Describe and predict interactions and effect between physical and cyber domains



Accomplishments:
- Sequoia HPC achieved world record 10^{15} events/sec
- Army: Cyber Army Modeling & Simulation (CyAMS)
- AF: Cyber Experimentation Environment

Technical Challenges:
- Automated, rapid instantiation of large-scale, complex computing and network environments
- Objective architecture for heterogeneous range component integration and synchronization
- M&S for large-scale aggregate Internet behavior, operating at multiple timescales
- Integrated high-fidelity models of kinetic and cyber phenomena
- Human behavioral and intention models
- Planning and Assessment algorithms to evaluate operational agility and assurance

Cyber CoI
5-Nov-2014 Page-16

Distribution A – For Public Release

**016 The modeling and simulation-- this is an area that's near and dear to my heart. It's actually a part of CERT's work that has always been important to understanding how do you interpret the real world in a way that you can model it and do reasoning about it, and also so that you can prevent it in training environments.

Being able to simulate the real world and being able to do experiments with human subjects is an important part of the work we do. You won't hear any human subject research here, but really understanding the role of humans is part of what we try and incorporate into modeling and simulation in terms of what we bring to the table, and you will hear a talk on how we assess people in

simulation environments, because a key challenge is you can't put the warfighter in harm's way in a warfighting situation and really effectively evaluate them. You want them to do their job then. But as part of training and assessment, you want to be able to understand what is your national capability from the Cyber Mission Force, for example, in terms of what real capability that you have there.

So, finally we're back to the agenda. Let me just make a few comments here before I go to questions on the talks here. The web traffic observation talk by Will Dormann will be-- it's about the foundations of trust. How do you know what a capability actually does? How do you assess that? Again, this is where we bring together the notion of research and our operational capability, because we've learned over the years someone can tell you what a system does but until you really look at the bits on the wire, you really look at what's happening on the CPU, you don't know, because people make design decisions, they make mistakes, and you'll see that in certain areas mistakes are being made at scale, and so I think you'll find Will's presentation very entertaining there.

For enhancing mobile security-- again, that's about trust. How do we make mobile devices? But it also ties into the tactical and mobile elements. The Cyber Vulnerabilities in Aviation Today-- that's where the Software

Engineering Institute's Chief Operating Officer, Bob Behler, will be talking about his experiences and his perspective as a test pilot. He's a retired two-star general, so I think you'll find that's where he can really pull together the warfighter needs and tie them into cyber. So that's about assuring effective missions.

Rhiannon Weaver's work on malware samples is really, again, coming back to this, "Let's look at the actual artifacts and see how they behave to understand how this affects the mission." We've got the resiliency panel that I've talked about before. Rotem's work on Automated Cyber-Readiness Evaluator, this ties into the modeling simulation and evaluating performers and operators, cyber mission forces, in situ for their effectiveness both individually and as a team. And then the DidFail analysis-- this is work that Lori Flynn and Will Klieber have been working on, in terms of how do you analyze the flow of information through malware applications-- I mean, through mobile applications. Maybe they're not too far apart-- but mobile applications to establish the trust of those systems. And finally we have the DevOps panel discussion, which, again, ties back into agility, this notion that the development environment is part of the Department of Defense's ability to agilely respond to adversaries.

So with that, Shane, I hope we have some questions, and we have a few minutes.

Shane McGraw: Great, we do. I got a question from Alex, asking, "Are you applying your research on platform IT cyber-physical systems? For example, aircraft, land vehicles, ships, etcetera?" It's actually a multipart question, so that's question one.

Greg Shannon: Okay. So cyber-physical systems is part of the embedded tactical challenge that it's facing. The good news there is that we have peer labs that are actually doing phenomenal work in this area-- MIT and Lincoln Labs, MITRE, Sandia National Lab and so on-- because that's been an area that's always been important in avionics, nuclear control systems. What's new in that space is that some of the more commercial capabilities in terms of sensors, industrial control systems. And so there's been a gap, and it's an area that we're looking at and investing in and figuring out how to work with our peers.

Shane McGraw: Part 2: "Have you evaluated the new risk management framework, RMF?"

Greg Shannon: So the great thing about the risk management framework is it's based on the resiliency management model that we've built over the last decade or so. So it's near and dear to our heart. It's a lighter version of our resiliency management model. But it positions us as key communicators, key promulgators of that capability, both for NIST into the broader

commercial space, but especially for the Department of Defense, that we can push forward that cyber risk framework type of assessment, because it's really part and parcel of work that we've been doing for over a decade.

Shane McGraw: Great. We had a couple questions asking about Greg's slides. We actually just added a PDF copy of the slides there now. So one of our breaks during the day, you want to log back out of the event and log back in and refresh, and the PDF copy will appear there. And then just the last part for Alex asking, "Are you working with architecture-centric model-based capabilities to evaluate systems before implementation?" He's working with Peter Filer and James Ivers on such efforts.

Greg Shannon: Sounds like a loaded question. Of course we are. But I mean, the real challenge there is how to incorporate the security aspects that are mission-relevant and appropriate threat model. So we've actually got other work in terms of trying to be more-- trying to advance the state of the art in threat modeling so that we can incorporate those into those architecture and make them more robust against the type of adversaries Department of Defense customers are actually facing.

Shane McGraw: Excellent. John wanted to know, "Is there a master's program in cybersecurity at CMU?" I know there's a CISO program at the Heinz school. Is there an actual master's?

Greg Shannon: Yeah, so the INI I believe has a number of cyber-related programs. They may not say cybersecurity specifically, but I know that they have a number of master's programs, and a number of staff here at CERT have come out of those programs, so they're more or less a cybersecurity program.

Shane McGraw: From Joseph, asking, "How can industry influence DoD research?"

Greg Shannon: This is an interesting question. DoD sees that defense industrial base industry as a key partner in defending the nation, but let me turn that around a bit. The Department of Defense would actually like to influence industry, because only the DoD can define what the national challenges are, what the threats to national security are, what the science and technology gaps are. And so they want to be able to effectively communicate that. That's a cornerstone element of the Reliance 21, of reaching out to industry and influencing industry in terms of what are the challenge problems, what are the needs, what are the measurements and metrics for capabilities in this area. But as always, most of the innovation comes out of-- or much of the innovation comes out of the commercial sector and the Department of Defense recognizes that.

Shane McGraw: Another tough question here from Don, asking, "Are there cyber experts and cyber

protections that offer 100 percent assurance of protection? If so, what are they?"

Greg Shannon: That's almost a philosophical question, and unfortunately probably not quite practical. We deal with risk every day; that's why the cyber risk framework is so important, and being able to make those tradeoffs is part of what we do. Can we do better to provide more assurance more efficiently? Yes, and that's why we continue the research.

Shane McGraw: One more from Joel, asking, "Is CERT attempting to reduce the acquisition lag to support timely adoption of emerging cyber concepts?"

Greg Shannon: We're certainly trying to inform the acquisition community about ideas about how to accelerate that process, but acquisition for cyber is seen as a really fundamental challenge that actually does affect national security because of the timelines.

Shane McGraw: Greg, excellent presentation. Thank you for kicking us off, giving an overview for the day.

Carnegie Mellon University

Carnegie Mellon University

This video and all related information and materials (“materials”) are owned by Carnegie Mellon University. These materials are provided on an “as-is” “as available” basis without any warranties and solely for your personal viewing and use.

You agree that Carnegie Mellon is not liable with respect to any materials received by you as a result of viewing the video, or using referenced websites, and/or for any consequences or the use by you of such materials.

By viewing, downloading, and/or using this video and related materials, you agree that you have read and agree to our terms of use (www.sei.cmu.edu/legal/).

© 2015 Carnegie Mellon University.

Copyright 2015 Carnegie Mellon University

Copyright 2015 Carnegie Mellon University

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the United States Department of Defense.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN “AS-IS” BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

This material has been approved for public release and unlimited distribution except as restricted below.

This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

Carnegie Mellon® is registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

DM-0002555

CERT | Software Engineering Institute | Carnegie Mellon University
CERT® Alignment with Cyber COI Challenges and Gaps
SEI Webinar
© 2015 Carnegie Mellon University