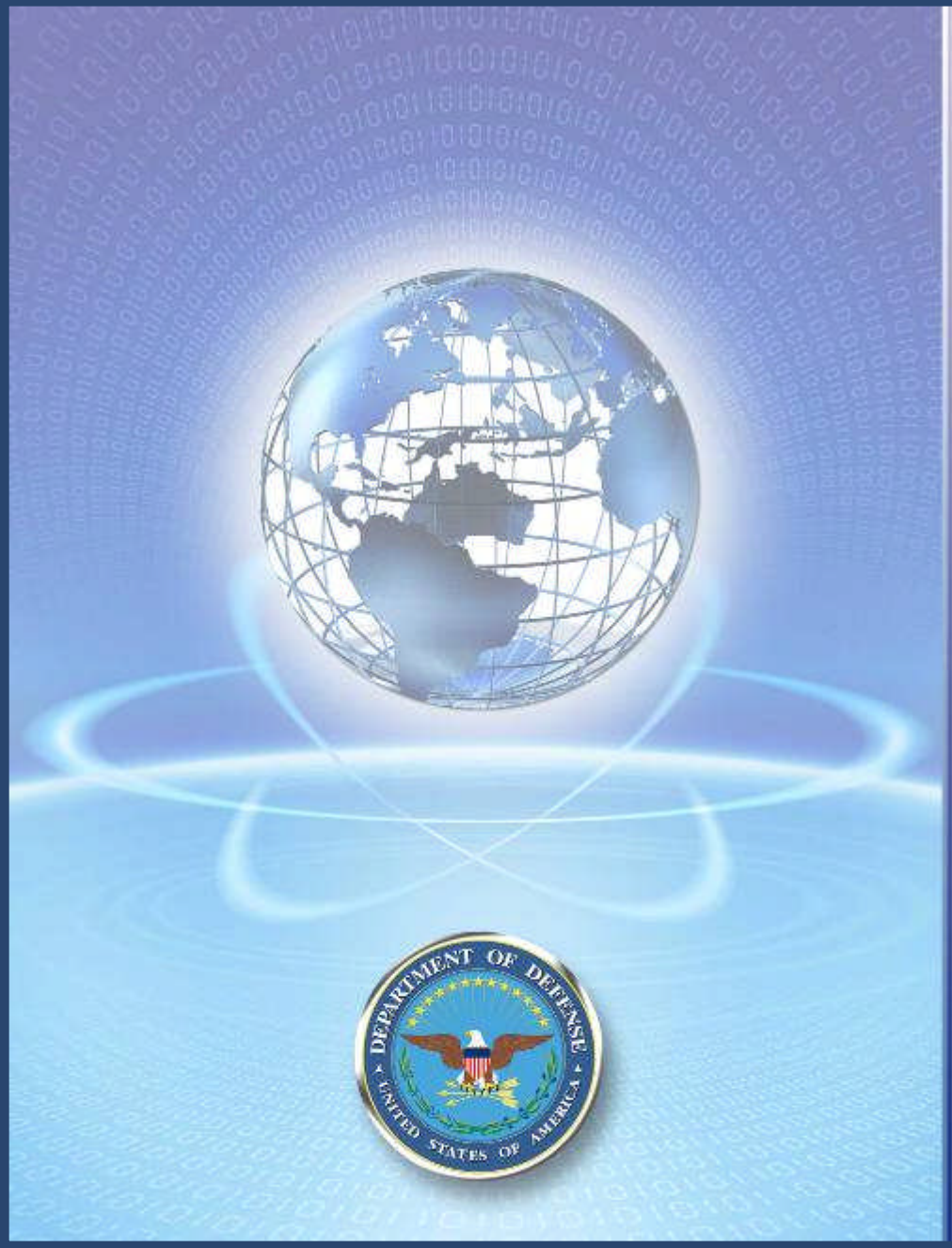


What's Next for Federal Cyber Security – A DoD Perspective

Mr. Gus Guissanie
Acting Deputy Assistant Secretary of Defense for Cyber, Identity and Information Assurance

Globalization Challenge

- Commercial IT functionality has penetrated nearly every aspect of mission critical functionality
- IP Convergence: IT communications connects mission critical functionality together with the functionality of the rest of the world
- IT Supply Chain has no borders

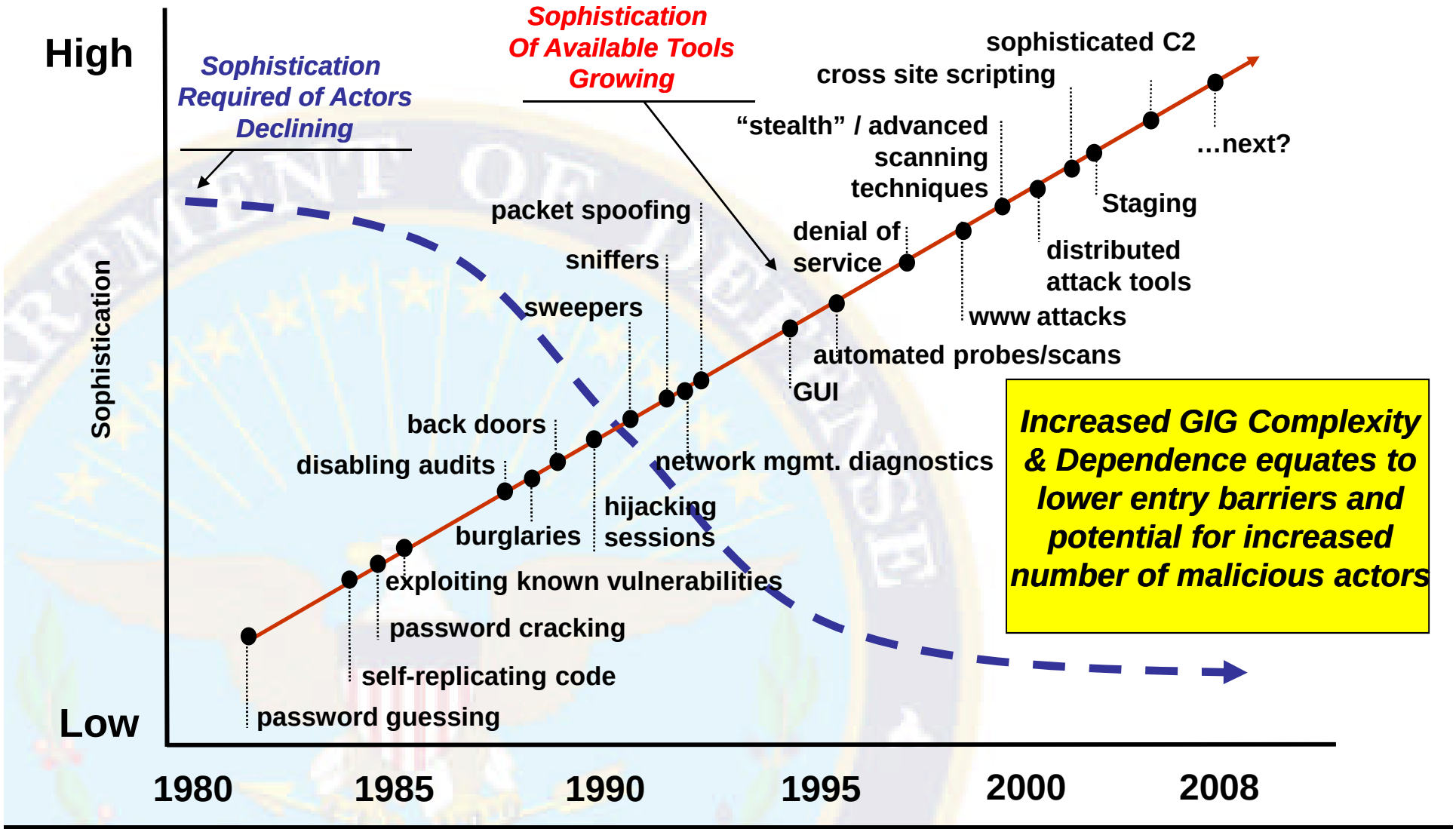
Net-Centric Convergence:

Allies and adversaries live and work on the same *commercial* sector networks

The Reality

The Cyber Domain is Hotly Contested

Defensive measures are outpaced by the well resourced sophisticated threat . . .



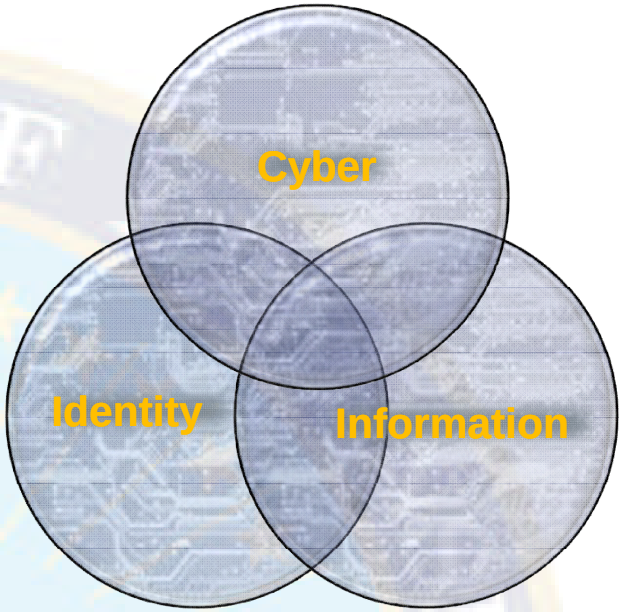
Sophisticated Adversaries

- Employ a full spectrum of offensive capabilities
  - Well resourced
  - Deep knowledge of latent vulnerabilities
  - Supply chain attacks to create vulnerabilities
- Don’t “play fair”
  - Use systems approach to identify target of attack
  - Wait for time and place convenient to themselves
- Individual target difficult to defend against determined sophisticated adversary case-by-case

Cybersecurity ➞ Mission Success

Cybersecurity - prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation. NSPD-54/HSPD-23

Cyber, Identity, and Information Assurance



Cyber – a domain of endeavor that creates a virtual interactive experience

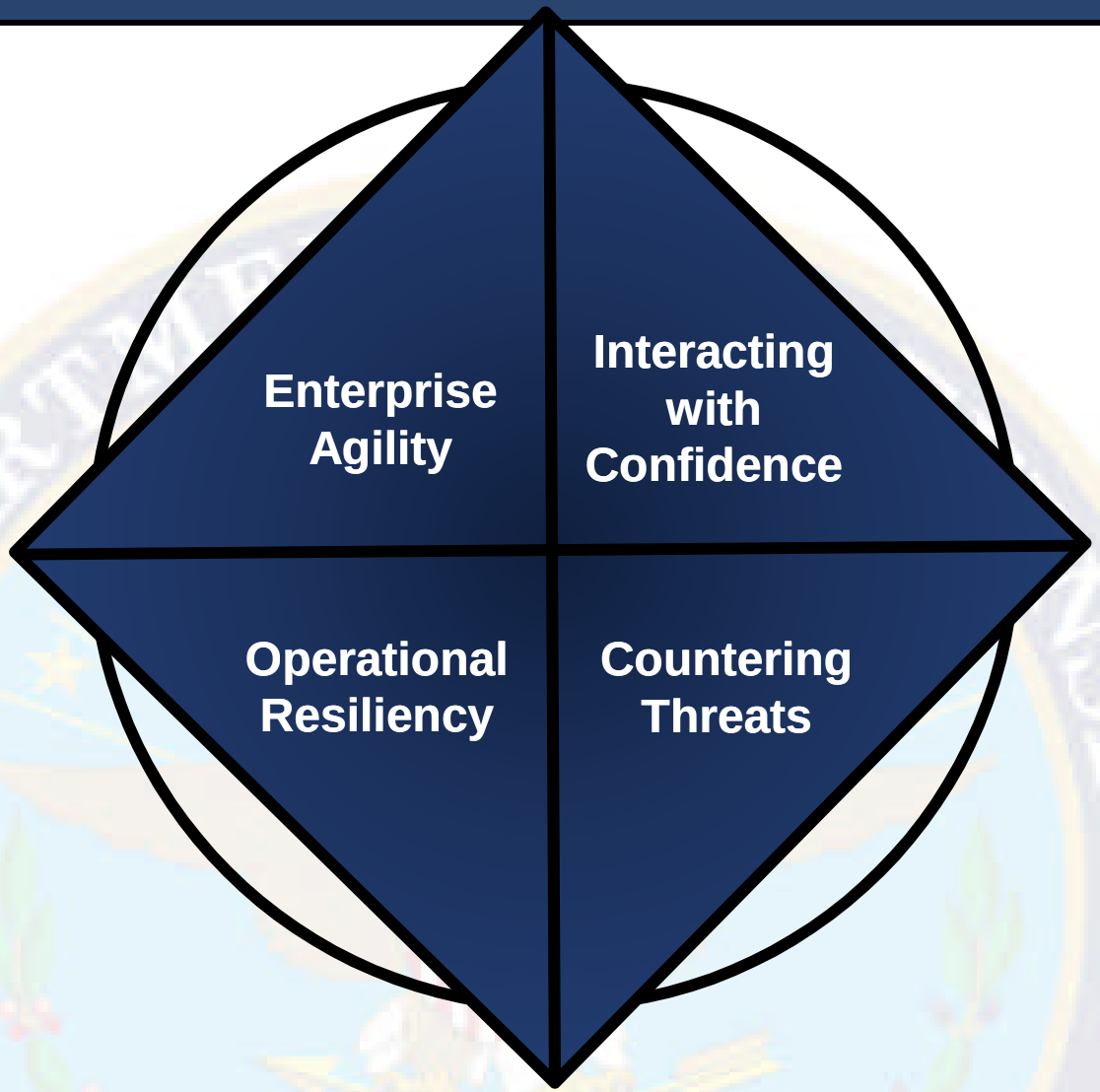
Identity – individuals, organizations, devices, assets

Information – content and services

Assurance

1. Is a **means** to guarantee or indemnify against loss due to a specified peril or contingency
2. Is confidence in means gained through **verification**
3. Provides **freedom of action** that arises from confidence in the means

Freedom of Action in Cyberspace

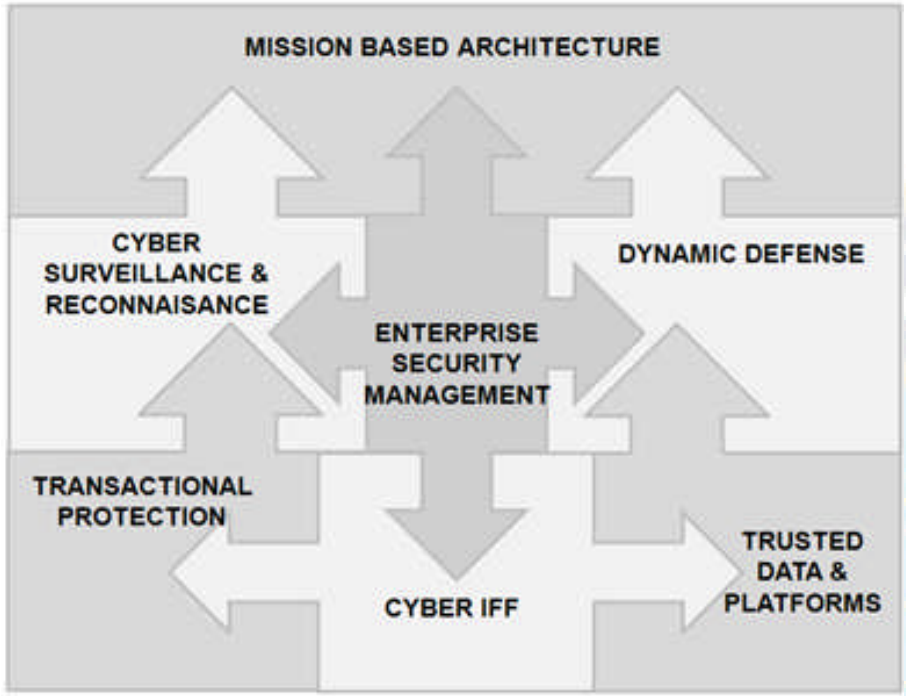


- The Defense information enterprise securely and seamlessly extends to mission partners.
- The Department has ready access to its information and command and control channels, and its adversaries do not.
- The cyber components of DoD weapons systems and other defense platforms perform only as expected.
- DoD cyber assets collectively, consistently, and effectively act in their own defense.
- Missions and operations continue under any cyber situation or condition.

Approach

Enterprise Agility	Interacting with Confidence	Countering Threats	Operational Resiliency
1	2	3	4
Organize for unity of purpose and speed of action	Enable secure mission-driven access to information and services	Anticipate and prevent successful attacks on data and networks	Prepare for and operate through cyber degradation or attack
1.1. Lead and Govern in an Uncertain Environment 1.2. Design for the Fight 1.3. Develop the Workforce 1.4. Partner for Strength	2.1. Secure Data in Transit 2.2. Manage Access 2.3. Assure Information Sharing	3.1. Understand the Battlespace 3.2. Prevent and Delay Attackers from Getting in the GIG 3.3. Prevent Attackers from Staying in or Acting	4.1. Develop and Maintain Trust in Data, Platforms and Networks 4.2. Strengthen Cybersecurity Readiness 4.3. Sustain Missions

Strategic CIIA Capabilities



Transactional Protection. End-to-end security controls for each information transaction in a variable trust environment.

Cyber Identification Friend-or-Foe (IFF). Enables distinction among friendly, neutral, and adversary cyber entities and ensures friendly cyber entities are visible, trackable, and addressable for management and control.

Trusted Data and Platforms. Integrity mechanisms to protect against attacks during manufacture or distribution (i.e., “supply chain”) and provide early warning and automated mitigation of data or platform degradation.

Cyber Surveillance & Reconnaissance. Persistent observation of GIG user, asset, and network behavior to detect anomalies, misuse, or unauthorized activity.

Enterprise Security Management. Integrated enterprise services for all security functions (e.g., identity, credential, attribute, policy, privilege, authentication, configuration, audit, and cryptologic key management).

Dynamic Defense Enterprise security management infrastructure linked to and alerted by extended cyber sensor networks that provide warning and response.

Mission Based Architecture. Networks, services, and data organized and optimized for mission availability.

Goal 1

Enterprise Agility

1

Organize for unity of purpose and speed of action

- **1.1. Lead and Govern in an Uncertain Environment**
- **1.2. Design for the Fight**
- **1.3. Develop the Workforce**
- **1.4. Partner for Strength**

1.1 **Lead and Govern in an Uncertain Environment.** *Provide vision and follow-through.*

1.2 **Design for the Fight.** *Deliver the right capabilities on the right time line. Synchronize and integrate capabilities across the enterprise.*

1.3 **Develop the Workforce.** *Provide a continuum of learning activities from* basic literacy to advanced specialties, recruit and retain highly qualified professionals in needed positions, and keep workforce capabilities current in the face of constant change.

1.4 **Partner for Strength.** *Leverage the unique capabilities of a wide set of partners to create advanced CIIA capabilities.*

Goal 2

Interacting with Confidence

2

Enable secure mission-driven access to information and services

- **2.1. Secure Data in Transit**
- **2.2. Manage Access**
- **2.3. Assure Information Sharing**

2.1 **Secure Data in Transit.** *Enable private information flows through robust, ubiquitous cryptographic services.*

2.2 **Manage Access.** *Enable secure, authenticated access among users, services, data, platforms and facilities based on mission needs. In this context, access includes visibility, configuration, connection and allocation, as well as authorization for use.*

2.3 **Assure Information Sharing.** *Enable secure, seamless information management and collaboration across information or security domains. Provide a full suite of secure sharing solutions for collaboration across networks, enclaves and COIs and with mission partners.*

Goal 3

Countering Threats

3

Anticipate and prevent successful attacks on data and networks

- **3.1. Understand the Battlespace**
- **3.2. Prevent and Delay Attackers from Getting in the GIG**
- **3.3. Prevent Attackers from Staying in or Acting**

3.1 **Understand the Battlespace.** *Align and benefit from audit, sensor, forensic and incident management inputs across the extended enterprise.*

3.2 **Prevent and Delay Attackers from Getting in the GIG.** *Apply knowledge of the network, vulnerabilities and adversaries to harden GIG entry and embrace tactics, techniques, and procedures that favor defenders.*

3.3 **Prevent Attackers from Staying in or Acting.** *Lower the value of an attack for the attacker and reduce the consequences of an attack for the Department. Detect malicious activity through passive sensors and active investigation. Reconfigure assets to foil attackers. Implement mechanisms that limit what the attacker can see, where they can go, or what they can control.*

Goal 4.1

4.1. **Develop and Maintain Trust in Data, Platforms, and Networks.** *Guarantee the continued integrity and availability of cyber assets, to include processors and controllers embedded in weapons systems or other defense platforms.*

4.1.1. **Assure for Use.** *Match supplier and product assurance to mission criticality and acquire products with assurance appropriate for use.*

4.1.2. **Engineer for Survivability.** *Ensure networks and services identified as critical are engineered to operate despite sophisticated cyber attack.*

4.1.3. **Maintain Integrity.** *Improve confidence that data and ICT components are sound at creation and remain so for as long as they are used.*

Operational Resiliency

4

Prepare for and operate through cyber degradation or attack

4.1. Develop and Maintain Trust in Data, Platforms and Networks

4.2. Strengthen Cybersecurity Readiness

4.3. Sustain Missions

Goal 4.2

4.2.1. **Enable Cyber Event Response.** *Link centers and operations across the extended enterprise and provide decision support for mission planning.*

4.2.2. **Exercise under Realistic Cyber Scenarios.** *Test procedures and tactics for work arounds and fall-backs in the face of hostility. Conduct periodic exercises or evaluations of the ability to operate in a "cyber-out" environment; that is, one that assumes loss of all cyber assets and connectivity.*

4.2.3. **Identify Critical Cyber Assets.** *Ensure a criterion exists for identifying cyber assets as critical and ensure assets meeting the criteria are so identified.*

4.2.4. **Improve Continuity Planning.** *Determine how missions will continue in the face of degraded or unavailable cyber assets, and establish priorities for restoration*.

Operational Resiliency

4

Prepare for and operate through cyber degradation or attack

4.1. Develop and Maintain Trust in Data, Platforms and Networks

4.2. Strengthen Cybersecurity Readiness

4.3. Sustain Missions

Goal 4.3

4.3.1. ***Respond to Cyber Events.*** *Assess cyber damage and prepare and execute courses of action for 'fighting through' adverse cyber effects.*

4.3.2. ***Sustain Mission Critical Functions under Degradation.*** *Dynamically allocate cyber resources as needed to sustain mission operations while addressing cyber failures, no matter the cause.*

4.3.3. ***Reconstitute Critical Cyber Assets.*** *Rapidly restore cyber assets to a trusted state to support ongoing mission operations.*

Operational Resiliency

4

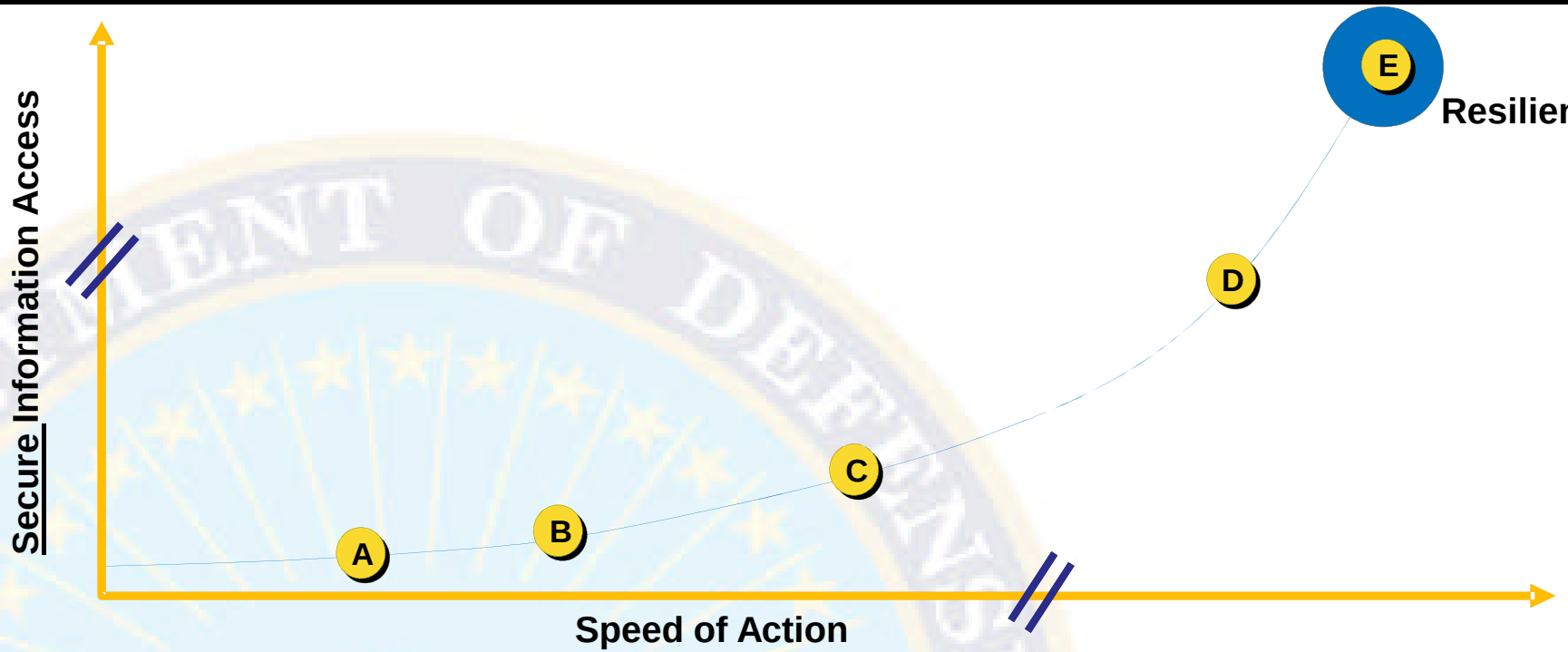
Prepare for and operate through cyber degradation or attack

4.1. Develop and Maintain Trust in Data, Platforms and Networks

4.2. Strengthen Cybersecurity Readiness

4.3. Sustain Missions

Toward a Resilient Cyber Ecosystem



A

Reactive & Manual

Security administrators follow rules and do their best to "put out fires"

B

Tools-Based

Tools and technologies are applied piecemeal to assist people in reacting faster

C

Interoperable

Loosely integrated tools exchange data to assist people with cyber situational awareness

D

Policy-Based

The enterprise instantiates security policy, illuminates events and helps the operators find, fix, and target for response

E

Resilient

Enterprise optimizes service to user by to dynamically isolating and containing effects – including in supply chain and underlying infrastructure

Questions?

Mr. Gus Guissanie
Acting Deputy Assistant Secretary of Defense for
Cyber, Identity and Information Assurance

Office of the Assistant Secretary of Defense for Networks
and Information Integration /
DoD Chief Information Officer
Department of Defense