

UNCLASSIFIED



# Developing a Sensing Strategy

Sylvia Mapes

Branch Chief, DISA, ID53

18 Jun 2015

United in Service to Our Nation  
UNCLASSIFIED

UNCLASSIFIED

# What is *sensing*?



**Sensing provides the means to *detect, interpret* and *correlate* electronic communications activity. Sensing in the context of cyber security includes both *network-based sensing* and *collection of log data* from hosts and devices.**

United in Service to Our Nation

UNCLASSIFIED

UNCLASSIFIED



## Why we need a sensing strategy

- **Unification of efforts toward common goal**
  - Consolidation, centralization, coordination
- **Shared understanding of the decision space**
  - The network we're defending, and the capabilities needed
- **Adaptability in the face of change**
  - The network, the threats, security technology

United in Service to Our Nation  
UNCLASSIFIED

UNCLASSIFIED

## BLUF: Key challenges today

- **Developing capability-oriented requirements**
  - Not lists of tools or product categories
- **Consolidation without losing capability**
  - Leaving sensors in place before replacements are deployed
  - Maintaining compatibility with legacy analysis systems (e.g., SIEM)
- **Complexity of managing different network appliances**
  - Many security appliances, separate from network devices
  - Complex technology dependencies, and immature technologies
- **Communication challenges to resolve these issues**
  - Complexity of stakeholders and their roles
  - Inability to resolve issues in a timely fashion

United in Service to Our Nation

UNCLASSIFIED

UNCLASSIFIED

# What we're defending

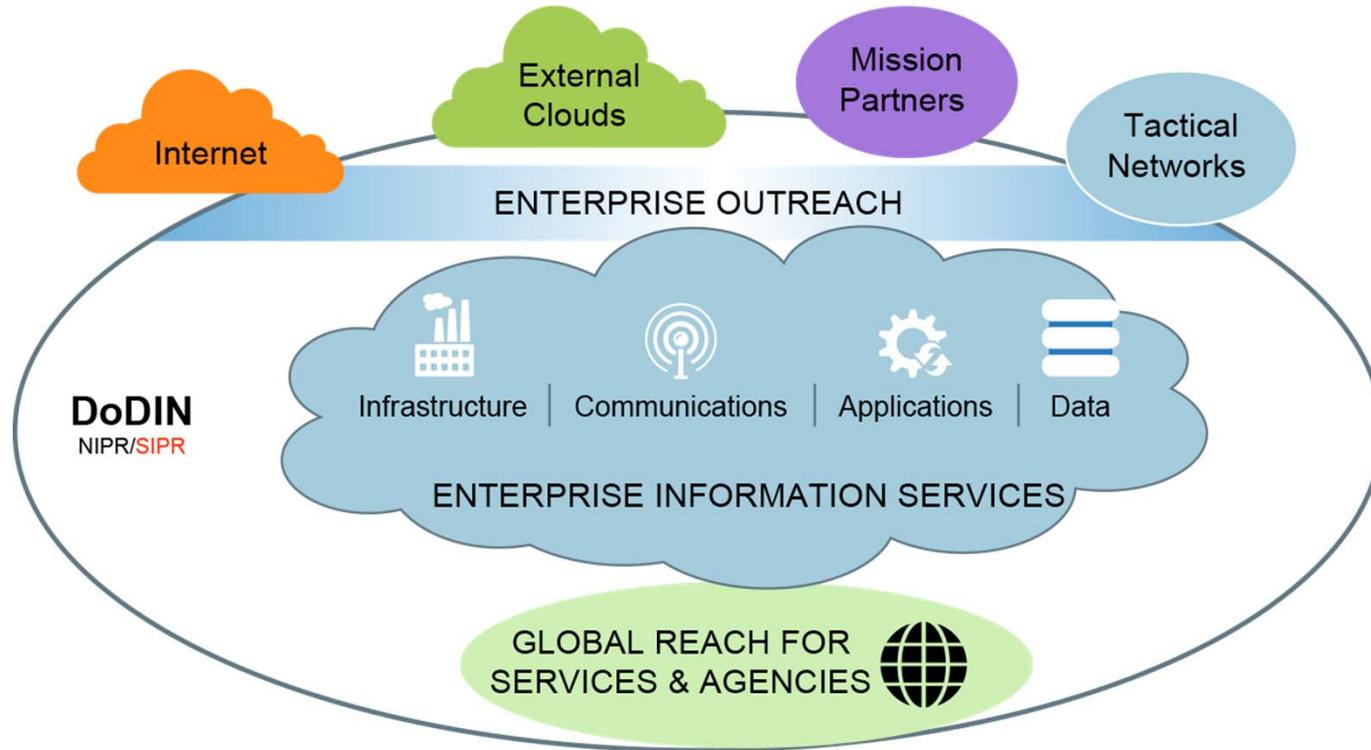
- **DISA-hosted enterprise services**
  - Defense Enterprise Email (DEE), Portal(DEPS), VOIP/Messaging (UC/DCS)
  - Bottom-line business driver for DISA
- **An evolving information and network architecture**
  - JIE – an information oriented architecture
  - JRSS - Robust, reliable network architecture
- **A network with a changing, elusive “perimeter”**
  - Mobility (DEM)
  - Hosting in the cloud
  - Cross domain, classified networks, multilevel security (MLS)

United in Service to Our Nation

UNCLASSIFIED

UNCLASSIFIED

# JIE – an ever evolving perimeter



United in Service to Our Nation  
UNCLASSIFIED

UNCLASSIFIED

# Our Approach



- **Approach our sensor strategy is like a business strategy**
- **Common language for communication is critical**
  - Define capabilities and locations – simplify and demystify.
- **Build an *architecture* to last**
  - Keep to some key design principles
  - Leverage current technology investments
- **Focus on our customers, the analyst user community**

United in Service to Our Nation  
UNCLASSIFIED

UNCLASSIFIED



# Capabilities, demystified



NETWORK SENSING

FULL  
Packet Capture

SECURITY EVENTS

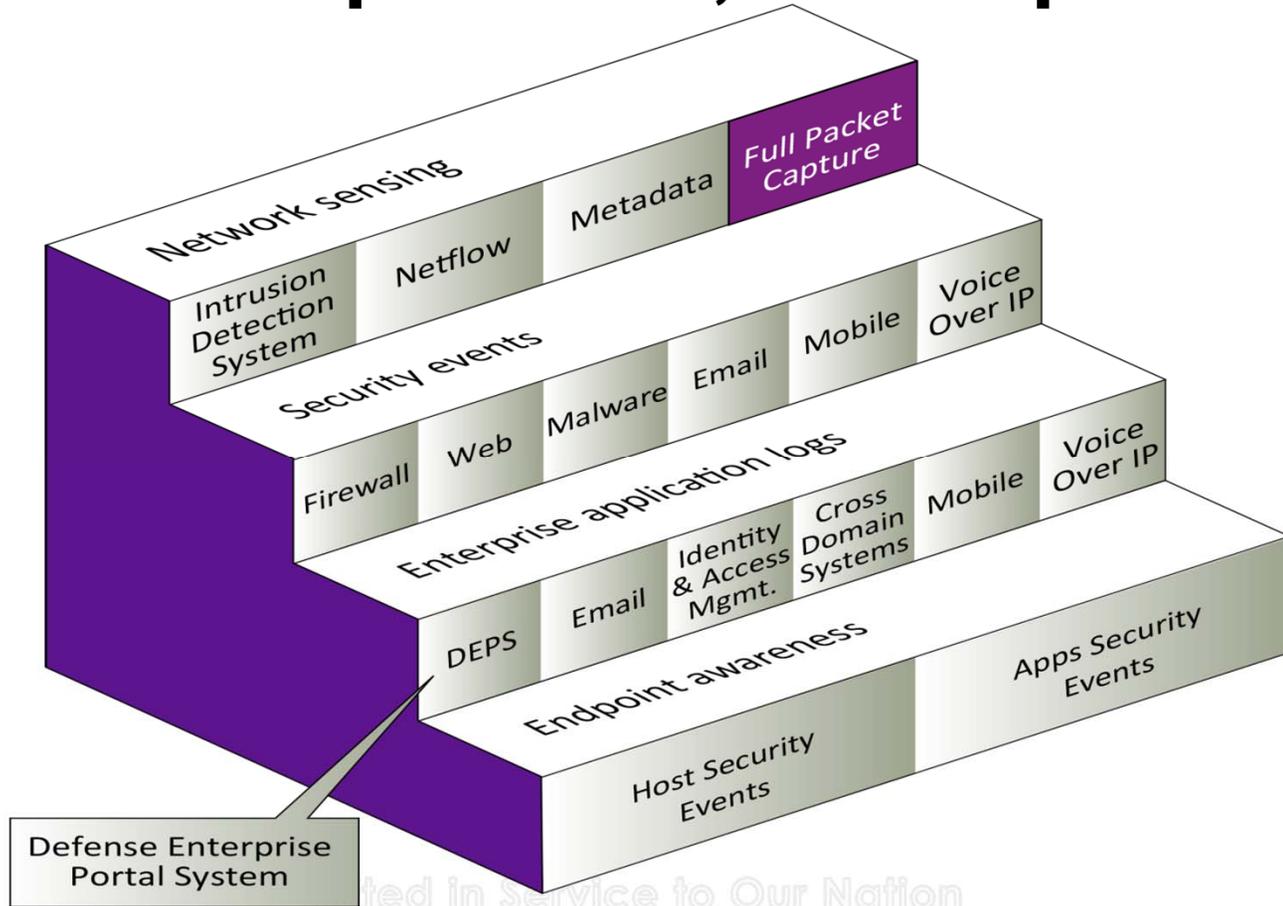
ENTERPRISE APPLICATION LOGS

ENDPOINT AWARENESS

United in Service to Our Nation  
UNCLASSIFIED

UNCLASSIFIED

# Capabilities, decomposed

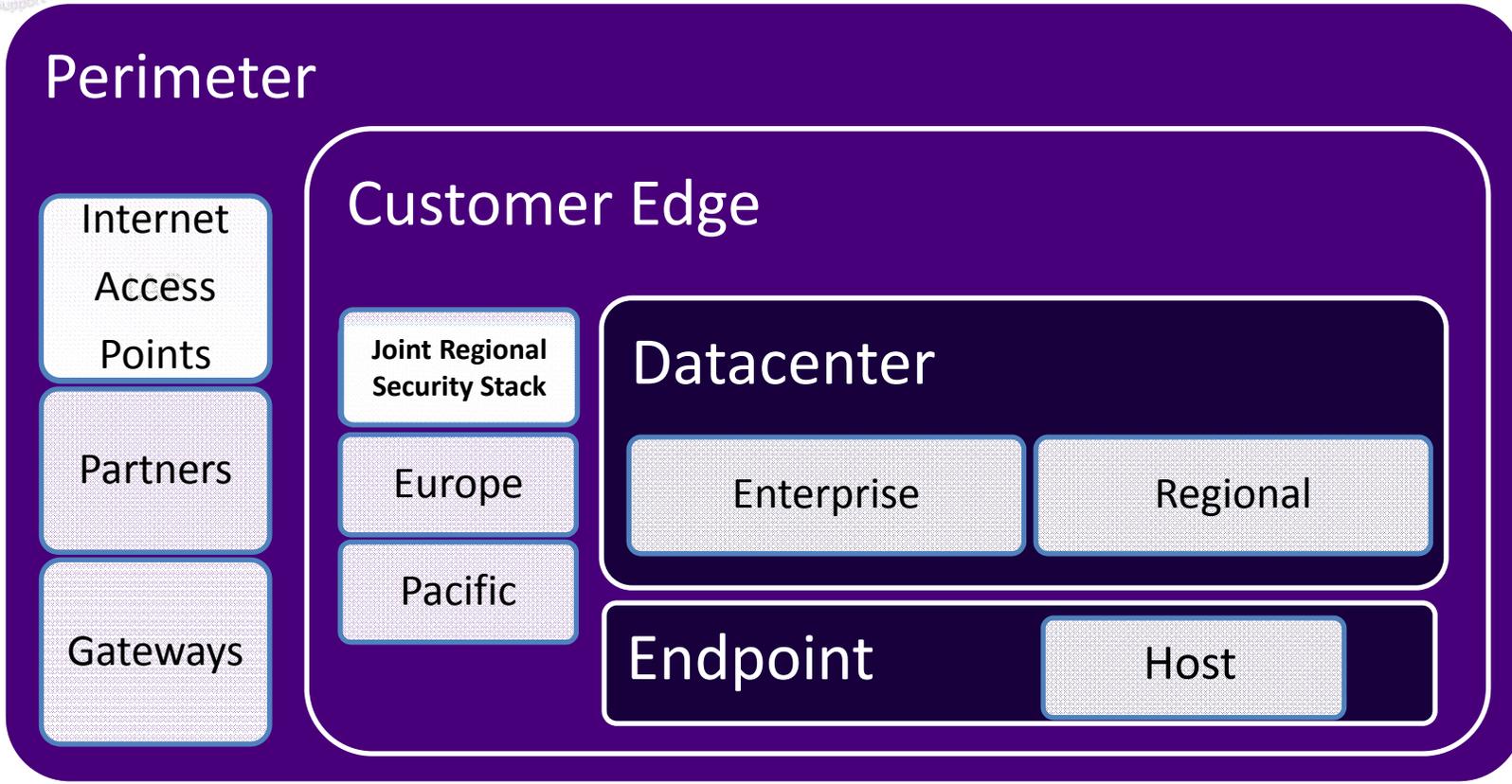


dedicated in service to Our Nation

UNCLASSIFIED

UNCLASSIFIED

# Sensing locations- demystified



United in Service to Our Nation  
UNCLASSIFIED

UNCLASSIFIED



# Location capability value matrix (notional data)

Location/ Capability	Network Sensing	Full Packet Capture	Security Events	Application Logs	Endpoint Security
Perimeter	HIGH	MEDIUM	HIGH	N/A	N/A
Customer Edge	MEDIUM	MEDIUM	HIGH	N/A	N/A
Datacenter	LOW	LOW	MEDIUM	HIGH	HIGH
Endpoint	LOW	LOW	LOW	MEDIUM	HIGH

United in Service to Our Nation  
UNCLASSIFIED

UNCLASSIFIED

# Key design principles

- **Maximize value**
  - Focus on blocking, reducing attack surface
  - Minimize false positives
  - Enable effective analyst work flows, automation
- **Minimize cost**
  - **Consolidate and reduce duplication**
    - Evaluate locations and capabilities
    - Consolidate without losing capability
  - **Total Cost of Ownership**
    - Control technical diversity
    - Understand total cost

United in Service to Our Nation

UNCLASSIFIED

UNCLASSIFIED

# We need your help



- **Government partners:**
  - Sensing capability consolidation is *hard*. It must be coordinated with changes to everything that depends on it.
  - We can't ignore O&M funding of legacy investments that fill a need not yet met by other technology.
  - Buy-in for this approach
- **Vendors:**
  - Integrated security and network devices
  - Standards development and adoption
  - Ease of deployment and management

United in Service to Our Nation

UNCLASSIFIED

UNCLASSIFIED



# Contact/POC Information

**Sylvia Mapes**

E-mail: [sylvia.t.mapes.civ@mail.mil](mailto:sylvia.t.mapes.civ@mail.mil)

Phone: 301-225-8758

**James Downey**

E-mail: [james.b.downey.civ@mail.mil](mailto:james.b.downey.civ@mail.mil)

Phone: 301-225-8673

**Vijay S. Sarvepalli**

E-mail: [vssarvepalli@cert.org](mailto:vssarvepalli@cert.org)

Phone: (703) 908-8332

United in Service to Our Nation

UNCLASSIFIED

UNCLASSIFIED

# United in Service to Our Nation



UNCLASSIFIED