Emerging Trends in Port Security

A.J. Briding
Senior Solutions Architect, CIBER, Inc.

AAPA New Orleans
2011

ciber Federal

Overview

- The Challenge
- Emerging Trends—The Big Picture
- Trend 1: Regionalization & Coordination
- Trend 2: Enterprise Integration
- Trend 3: Cybersecurity

ciber Federal

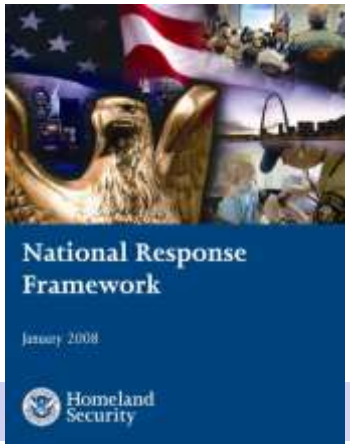
The Challenge

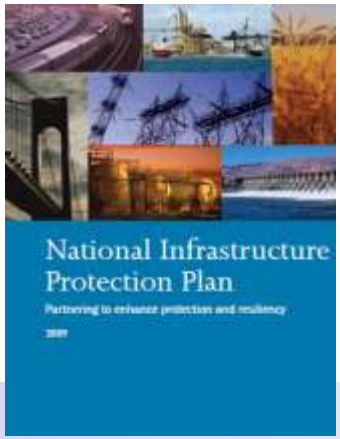
- Normal port operations
- Access control
- Cargo scanning and security
- Port security
- Maritime Domain Awareness
- Continuity of operations and resumption of trade
- Interagency coordination
- Limited budget and resources
- Legacy systems
- Cybersecurity

ciber Federal

Emerging Trends—The Big Picture

- DHS Policies
  - National Response Framework (NRF)
    - Integration of federal, state, local, and private sectors
  - National Infrastructure Protection Plan (NIPP)
    - Sector-specific critical infrastructure guidance
    - Port Security Grant Program emphasis areas
  - Comprehensive National Cybersecurity Initiative (CNCI)
    - Supply-chain risk management and critical infrastructure





The Comprehensive National Cybersecurity Initiative

ciber Federal

Emerging Trends—The Big Picture (cont.)

- Business Drivers
  - Economic viability
  - Multi-function systems
  - Limited IT budgets
- Operational Imperatives
  - Effective port operations
  - Effective and timely situational awareness and response
  - Smooth transition to emergency operations
  - Right information to the right people under all conditions

ciber Federal

Emerging Trends—The Bottom Line

- Securing critical infrastructure such as ports from both physical and cyber attack
- Coordination between federal, state, regional, local, and private sector agencies for situational awareness, response, and recovery capabilities
- Seamless integration of normal and emergency operations

ciber Federal

Trend 1: Regionalization & Coordination

- Many potential security partners
  - Sector command centers (SCCs)
  - Joint Harbor Operations Centers (JHOCs)
  - Regional emergency management agencies (EMAs)
    - Urban Areas Security Initiative (UASI) regions
    - Municipal EMAs
  - Security and response agencies
    - Harbor police
    - Municipal police, fire, EMS
    - County agencies
    - State and federal agencies

-- *Necessity to tailor coordination to each port*

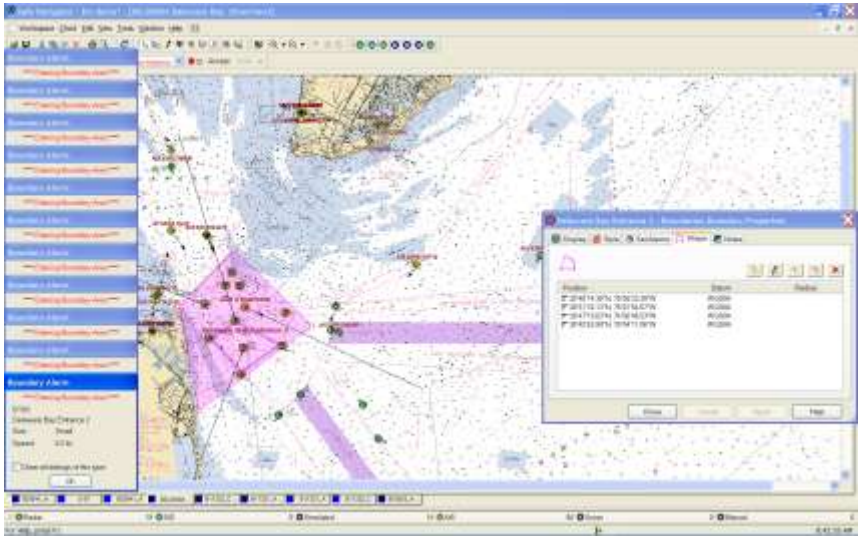
Trend 2: Enterprise Integration

- Stand-alone (point) solutions less effective, increase expense
- Separate normal and emergency operations systems sub-optimal
  - Drives up expense, maintenance, training
  - Lowers responsiveness and effectiveness
- Same subsystems common to both normal and emergency ops
  - Situational awareness, command and control
- Sensor fusion, intelligence fusion, comprehensive Common Operating Picture (COP)

ciber Federal

Technology Solution: PSIM Platforms

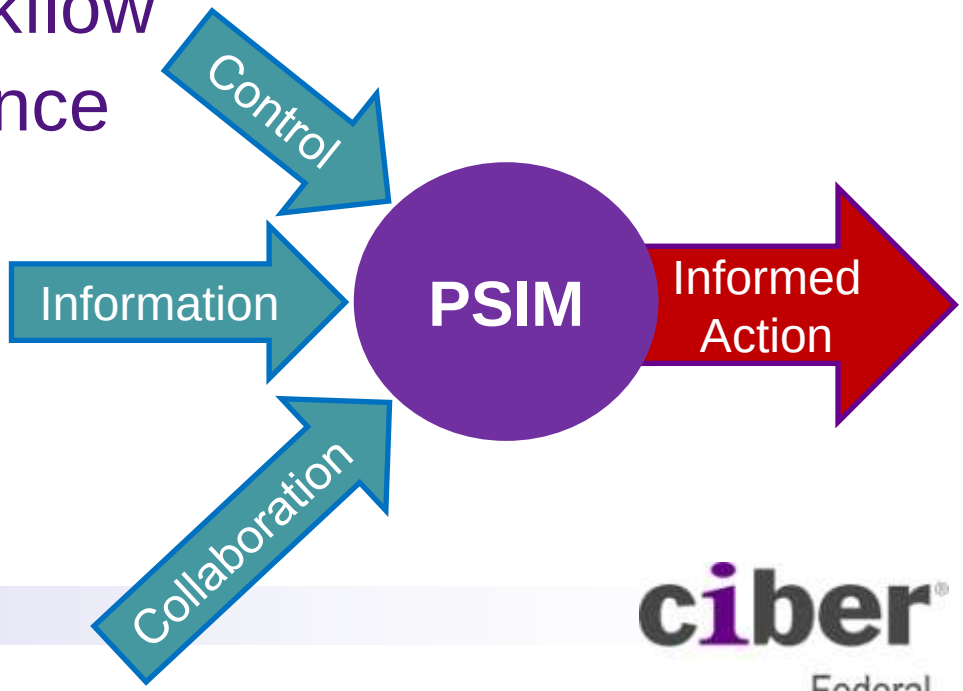
- Physical Security Information Management (PSIM)
  - Manage disparate systems from one platform
  - Integrate separate security systems into a single COP
  - Coordinate with multiple agencies
  - Provide intelligent workflow



ciber Federal

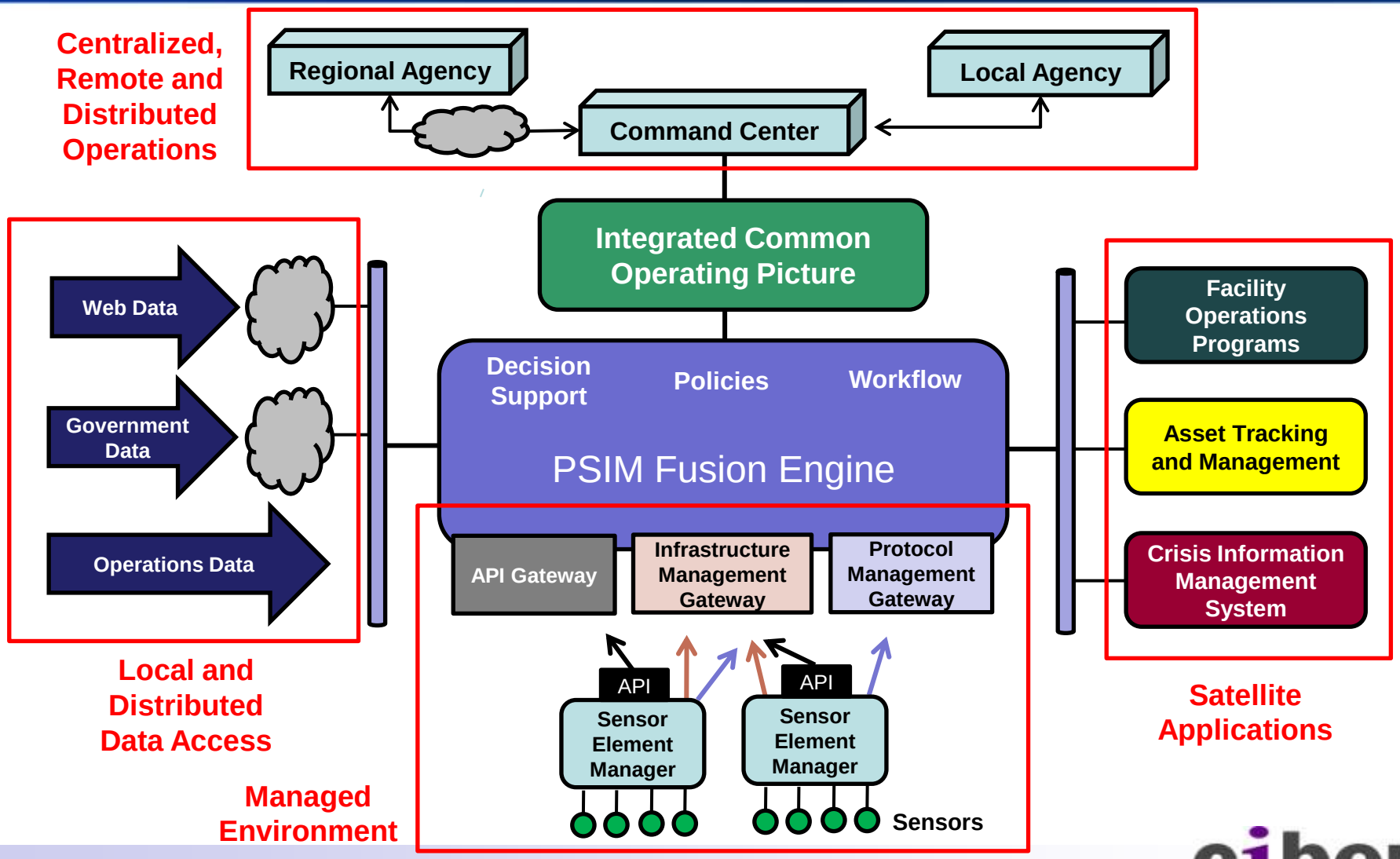
PSIM Qualities

- Integrated data collection
- Intelligent analysis and correlation
- Real-time situational awareness and decision support
- Intelligent process workflow
- Reporting and compliance
- Vendor independent



ciber Federal

The PSIM Enterprise Solution



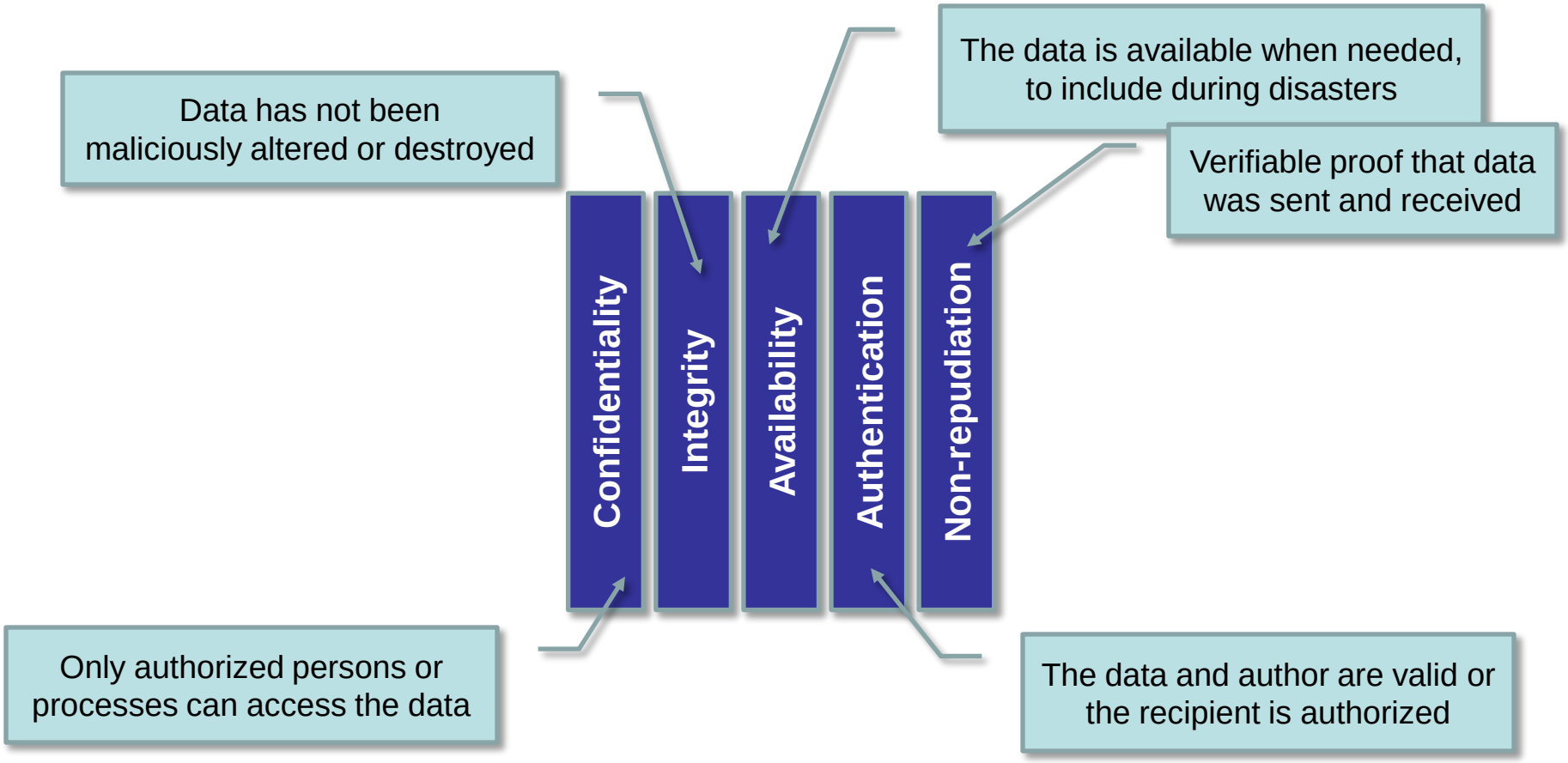
ciber Federal

Trend 3: Cybersecurity

- Synonymous with Information Assurance (IA)
- Basic elements:
  - Availability, integrity, authentication, confidentiality, and non-repudiation of information and information systems
  - Includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities

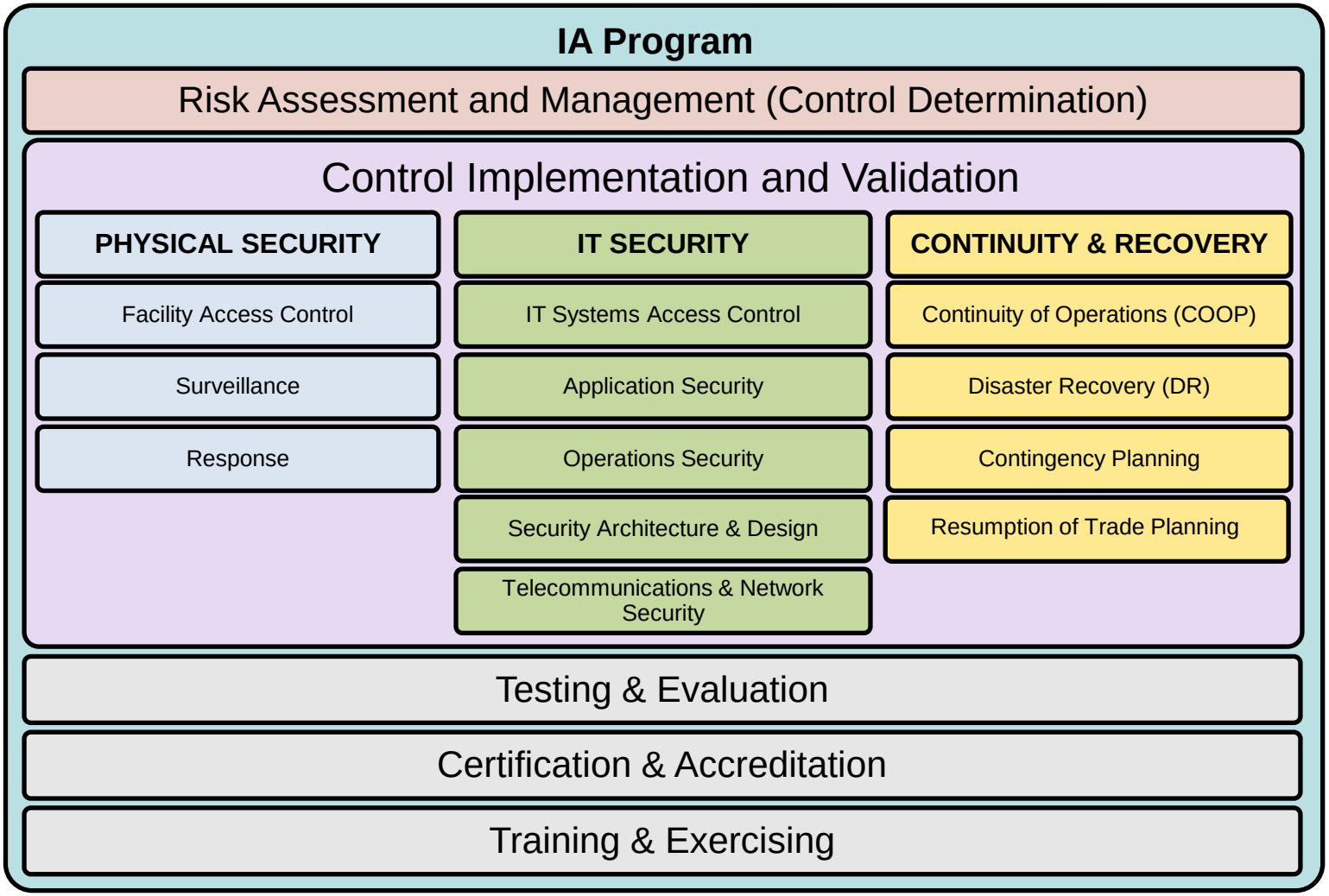
ciber Federal

The Five Pillars of Cybersecurity (IA)



ciber Federal

It Takes Much More than IT Security



ciber Federal

Cybersecurity Measures

- Build security standards into products
- Use enterprise approach
  - As strong as the weakest link
- Apply comprehensive risk management to identify and tackle biggest issues
- Refer to National Institute of Standards and Technology (NIST) security control standards for comprehensive approach

ciber Federal

PSGP Authorized Equipment List

[05] Cyber Security Enhancement Equipment

- [05AU-00-BIOM] Device, Biometric User Authentication
- [05AU-00-TOKN] System, Remote Authentication
- [05EN-00-ECRP] Software, Encryption
- [05EN-00-ETRN] Encryption, Data Transmission
- [05HS-00-FRNS] Software, Forensic
- [05HS-00-MALW] Software, Malware Protection
- [05HS-00-PFWL] System, Personal Firewall
- [05NP-00-FWAL] Firewall, Network
- [05NP-00-IDPS] System, Intrusion Detection/Prevention
- [05NP-00-SCAN] Tools, Network Vulnerability Scanning
- [05NP-00-SEIM] System, Security Event/Incident Management
- [05PM-00-PTCH] System, Patch/Configuration Management

ciber Federal

Emerging Trends in Port Security

A.J. Briding
Senior Solutions Architect, CIBER, Inc.

ciber Federal