NORTHROP GRUMMAN

PSCR 2010 Winter Conference

Access, Cyber Threat, and Identity Management

Mark Adams

Northrop Grumman Information Systems
Director, Networks and Communications
Office of the Chief Technology Officer

December 2, 2010

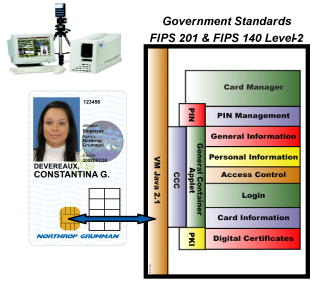
NGC's IDM PIV-I Approach – Current State

NORTHROP GRUMMAN

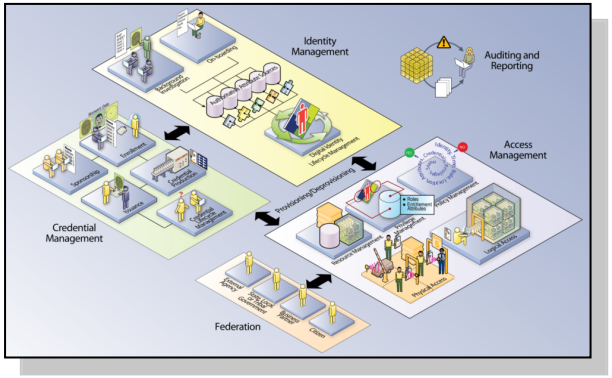
NGC Federated Common Identity Policy:

- **Smart Card & Electronics (GSA Certified)**
  - FIPS 201 (SP 800-85B) Electronics Testing
  - PIV 2 - Applets & Middleware
  - Auditor - OMB / Card & Electronics
- **FIPS 201 Process Lifecycle (ATO)**
  - Stakeholders, Process, Training (SP 800-79, 800-53/53A)
  - All FIPS 201 (GSA ABL) Compliant equipment
  - Auditor – Electrosoft (GSA's Agency Auditor)
- **CertiPath PKI (Certified)**
  - Cross certified to Federal Bridge
  - Bi-Lateral Trust with DOD (JITC)
  - Auditor – DoD's PKI Auditor
- **Key Recovery Practice Statement (KRPS) (Certified)**
  - Cross certified to Federal Bridge
  - Direct Bilateral Trust with DOD (JITC)
  - Auditor – DoD's PKI Auditor

Components & Infrastructure:



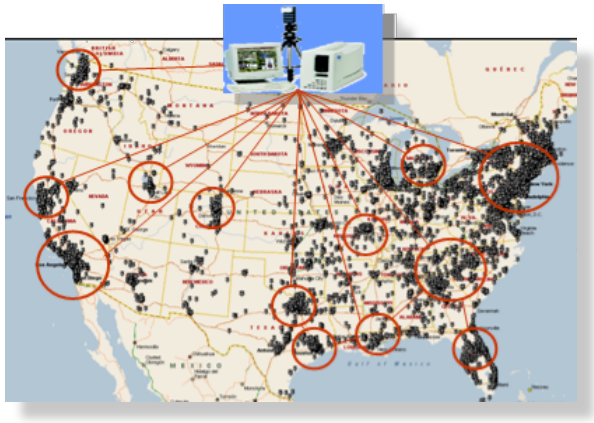
ICAM Architecture



IDM Solutions:

A single device that supports multiple authentication methods and enforces IDM polices across the enterprise

- ***Key Features***
  - Layered Technology Approach (When contract or security requires)
  - One Time Password (Remote Access)
  - Cross Certified CertiPath Certificate (Replacement of ECA Certificates)
  - Desktop Middleware (2 or 3 factor Authentication)
  - Single Sign-on (Password Vault)



Autumn Blend Exercise

CAC / PIV / PIV-I eValidation Process

Federal

SLTT

CIKR

Volunteers

Standard enables process to include:

1. D S C A
2. Mutual aid agreement
3. Business continuity agreements

Paper-based, visual or FIPS 201 eValidation to include:

1. ID (2 forms if visual)
2. Attribute or Affiliation
3. Deployment Source Authority

JRSOI

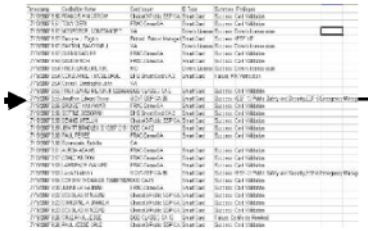
JRSOI = Joint Receiving Staging Operations Integration

Contingency Relocation or Response / Recovery Locations

Provides a real-time roster

Access Data:

- accountability
- traceability
- liability



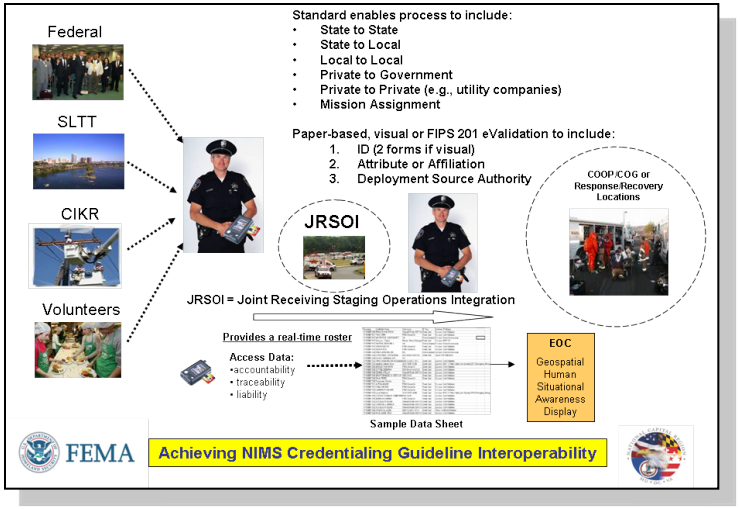
Sample Data Sheet

EOC

Geospatial Human Situational Awareness Display

Next Steps: Information Assurance and Secure Collaboration "Illustrative" Full Scale Federated Exercise

- **Strategic Goals**
  - **NSTIC GOALS 1, 2 & 3:**
    - Develop a comprehensive Identity Ecosystem Framework
    - Build and implement an interoperable identity infrastructure aligned with the Identity Ecosystem Framework
    - Enhance confidence and willingness to participate in the Identity Ecosystem
  - **TSCP GOAL 1 & 3:**
    - Enable secure information sharing within and between industry and governments
    - Define interoperable specifications and solutions that enable re-use in a cost-effective manner across multiple programs
- **Business Case**
  - **Federated Common Identity Policy:** TSCP Policies and Specifications align with DOD and Federal Identity Policies
  - **Multi-Factor Security:** Multi-Factor approach to provide additional security layers across our networks, systems, facilities, data, intellectual property and information assets
  - **Cost Control and Recovery:** Enterprise cost savings through enterprise deployment of TSCP Specifications while at the same time recover the cost of our investments
- **Sample Use Case Scenarios Include:**
  - ✓ **Use Case 1:** Identity interoperability (federation) of multi-level identity authentication across government & company domains
  - ✓ **Use Case 2:** Identity Authentication at emergency venues to positively and securely authenticate authorized users for logical & physical access
  - ✓ **Use Case 3:** Employees of critical businesses who work and/or reside in the impacted areas
  - ✓ **Use Case 4-6:** Disaster Recovery, Pandemic & Cyber Threats Exercise



Potential Partners include:

- ✓ **TSCP member Companies**
- ✓ **DOD**
- ✓ **Department of Homeland Security**
- ✓ **FEMA**
- ✓ **State of Virginia (Governors Office)**
- ✓ **City of Newport News (VA)**
- ✓ **City Hampton Roads (VA)**
- ✓ **District of Columbia - Metro**
- ✓ **State of Illinois**
- ✓ **City of Chicago**
- ✓ **Port of Chicago, O'Hare Airport**
- ✓ **N.Y. Port Authority**
- ✓ **NIST (700 MHz Test Bed)?**

Transglobal Secure Collaboration Program (TSCP)

- Government-industry partnership specifically focused on mitigating the risks related to compliance, complexity, cost and IT that are inherent in large-scale, collaborative programs that span national jurisdictions.

- To do business in the world today, A&D companies must balance the need to protect intellectual property (IP) while demonstrating willingness and ability to meet contractual requirements from government customers for auditable, identity-based, secure flows of information.

Common Framework for Federated Collaboration

- **Identity Management & Information Assurance:**
  - Provide assurance that collaborative partners can be trusted
  - Meet government agencies' emerging requirements for identity assurance across domains
  - Establish common credentialing standards that accommodate and span national jurisdictions
  - Protect personal privacy data of employees
- **Data Protection:**
  - Define fine grain access right attributes for data labeling and data right's management
  - Establish "Application Awareness"
  - Demonstrate compliance with export control regulations
  - Protect corporate IP in collaborative and other information sharing programs
- **Facilitate Secure Collaboration:**
  - Provide collaborative toolsets that will interoperate with customers and suppliers
  - Facilitate re-use collaborative capabilities among multiple programs

Contact:
Keith Ward
Email: k.ward@ngc.com

Mark Adams
Email: ms.adams@ngc.com