No More Excuses:
Feds Need to Lead with Strong Authentication!

Dr. Sarbari Gupta

Electrosoft

sarbari@electrosoft-inc.com

Annual NCAC Conference on Cybersecurity

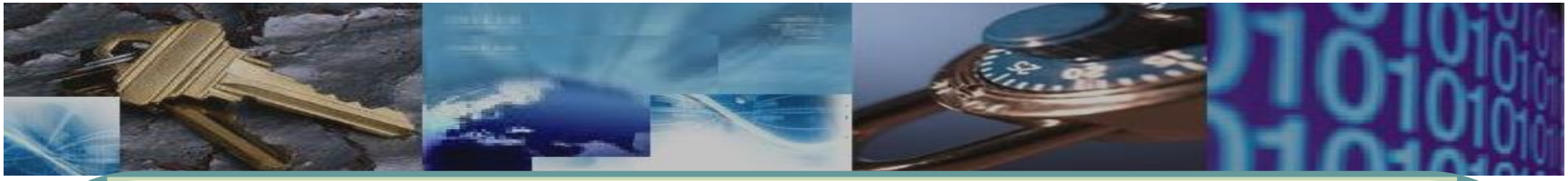
March 16, 2016

Electrosoft Services, Inc.
1893 Metro Center Drive
Suite 228
Reston, VA 20190

Web: http://www.electrosoft-inc.com
Email: info@electrosoft-inc.com
Tel: (703) 437-9451
FAX: (703) 437-9452

Agenda

- The Problem
- Terms and Concepts
- Policies and Regulations
- Current Status
- Challenges
- Way Forward



- **The Problem**
  - ***Root cause of many recent breaches is "weak authentication"***

Breaches – Large Retailers

- **Home Depot (2014)**
  - ***56 Million credit/debit cards compromised***
  - ***Network penetrated using stolen credentials from Vendor***
  - ***Installed custom-malware to steal customer information***
- **Target (2014)**
  - ***40 Million credit/debit cards compromised***
  - ***Network break-in using stolen credentials from HVAC contractor***
- **Neiman Marcus (2016)**
  - ***5200 Accounts compromised***
  - ***Automated attacks on username/password combinations to obtain unauthorized access***
- **Sony (2014)**
  - ***Phishing emails to steal credentials and personal information***
  - ***Penetrated other accounts (weak password policy)***

Breaches - Federal Government

- **Internal Revenue Service (IRS) - 2015, 2016**
  - ***100,00 taxpayer accounts exposed***
  - ***Personal data portfolios built to hack Knowledge Based Authentication (KBA) authentication***
- **US Postal Service (USPS) - 2014**
  - ***Personal data of 800,000 USPS employees exposed***
  - ***Weak VPN authentication mechanisms suspected as being attack pathway***
- **Office of Personnel Management (OPM) - 2015**
  - ***Personnel data of 4.2 million Federal staff exposed***
  - ***Background investigation data for 21.5 million individuals stolen***
  - ***Hackers infiltrated network using credentials stolen from Government contractor***

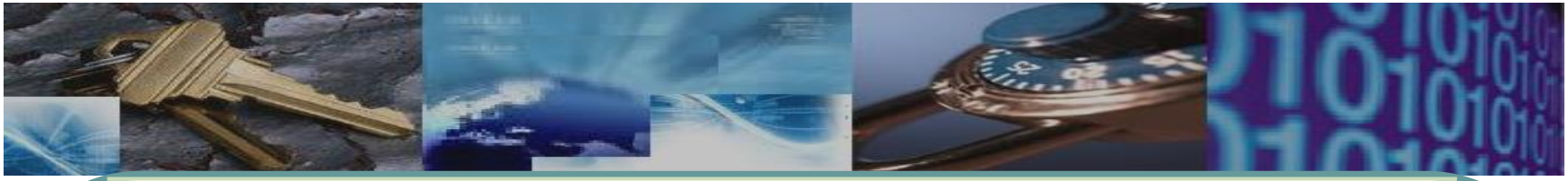
Passwords are “broken!”

- **Passwords are the de facto method of authentication – Why?**
  - ***Easy to use***
  - ***Low cost to set up (very expensive to maintain!)***

- **Passwords are “broken” – Why?**
  - ***Easy to guess***
  - ***Easy to “crack” with available tools***
  - ***Easy to share or steal***
  - ***Easy to forget***
    - **Leads to “sticky notes”**
    - **Leads to heavy help desk costs**

National Strategy for Trusted Identities in Cyberspace(NSTIC)

- **NSTIC issued in April 2011**
  - ***Focus on "killing" the password!***
  - ***Encourages collaboration between public and private sectors to raise level of trust associated with identities involved in online transactions***
- **Guiding Principles: Identity solutions will be:**
  - ***Privacy-enhancing and voluntary***
  - ***Secure and resilient***
  - ***Interoperable***
  - ***Cost-effective and easy to use***



- **Terms and Concepts**
  - ***Authentication is a Critical Component of Effective Cybersecurity***

Authentication Basics

- **Identification**
  - ***The process of declaring a claimed identity***
- **Authentication**
  - ***"The process of establishing confidence in the identity of users or information systems" [SP 800-63-1]***
  - ***Three widely accepted factors of authentication:***
    - **Something you know (e.g., secret or passphrase)**
    - **Something you have (e.g., a key or badge)**
    - **Something you are (e.g., fingerprint or facial image)**
  - ***Strong Authentication***
    - **Uses two or more factors**
- **Authorization**
  - ***Focused on "identifying the person's user permissions" [M-04-04]***

Identification, Authentication and Authorization

Hi, my name is Sam Jones! (Identification)

Please show me your Drivers License

Here it is, Officer!

OK. The license looks legitimate and I see your picture and name on it. (Authentication)

I am authorized to drive trucks.

I see you have a Commercial Drivers License. Have a great day! (Authorization)

OK. Thank you, Officer!

If not passwords, then what?

- **Passwords**
  - ***Weak (single factor) authentication***
  - ***Two passwords in sequence is still considered single factor***
- **Strong Authentication (Multifactor)**
  - ***Smart card with PIN activation***
  - ***Smart card with biometric activation***
  - ***Password plus One Time Code (via mobile)***
  - ***Many more …***

Authentication – Critical to Security

- **NIST SP 800-53 Rev 4**
  - ***Identification and Authentication is ONE of EIGHTEEN control families***
  - ***However, it is a foundational element of cybersecurity!***

 # From NIST SP 800-53 Rev 4

TABLE 1: SECURITY CONTROL IDENTIFIERS AND FAMILY NAMES

ID	FAMILY	ID	FAMILY
AC	Access Control	MP	Media Protection
AT	Awareness and Training	PE	Physical and Environmental Protection
AU	Audit and Accountability	PL	Planning
CA	Security Assessment and Authorization	PS	Personnel Security
CM	Configuration Management	RA	Risk Assessment
CP	Contingency Planning	SA	System and Services Acquisition
IA	Identification and Authentication	SC	System and Communications Protection
IR	Incident Response	SI	System and Information Integrity
MA	Maintenance	PM	Program Management

NIST 800-53 Rev 4 - Control IA-2

- **IA-2: Identification and Authentication (Organizational Users)**

- **Control Statement:**
  - ***The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).***

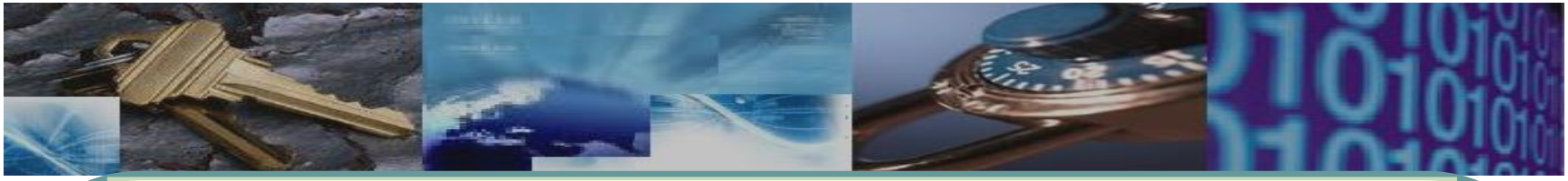
- **Control Enhancements:**
  - ***(1) The information system implements multifactor authentication for network access to privileged accounts.***
  - ***(2) The information system implements multifactor authentication for network access to non-privileged accounts. [MOD, HIGH]***
  - ***(12) The information system accepts and electronically verifies Personal Identity Verification (PIV) credentials.***

NIST 800-53 Rev 4 - Control IA-8

- **IA-8: Identification and Authentication (Non-Organizational Users)**

- **Control:**
  - ***The information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users).***

- **Control Enhancements:**
  - ***(1) The information system accepts and electronically verifies Personal Identity Verification (PIV) credentials from other federal agencies.***
  - ***(2) The information system accepts only FICAM-approved third-party credentials for organizational information systems that are publicly accessible to the general public.***



- **Policies and Regulations**
  - ***Requirements for Federal Agencies are already well-established!***

HSPD-12 and PIV

- **HSPD-12: Policy for a Common Identification Standard for Federal Employees and Contractors (2004)**
  - ***Policy to establish a mandatory, Government-wide standard for secure and reliable forms of identification***
  - ***To be issued by the Federal Government to its employees and contractors***
  - ***To enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy***
- **FIPS 201: Personal Identity Verification (PIV) of Federal Employees and Contractors (2005)**
  - ***Standard established by NIST***
  - ***Smart card based identity credential***
  - ***Testing program established by GSA***

OMB Policy Memos - Authentication

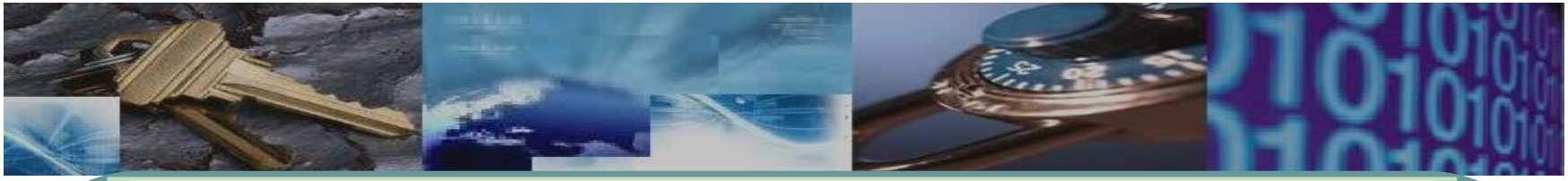
- **M-05-24: Implementation of HSPD-12 (2005)**
  - ***Requires Agencies to conduct background investigation and issue identity credentials to employees / contractors***
- **M-07-06: Validating and Monitoring Agency Issuance of PIV Credentials (2007)**
  - ***Requires quarterly reporting of PIV Card issuance***
- **M-11-11: Continued Implementation of HSPD-12 (2011)**
  - ***Plan to expedite the full use of the PIV credentials for access to federal facilities (physical access) and information systems (logical access)***

CAP Goal - Cybersecurity

- **14 Cross Agency Priority (CAP) Goals**
  - ***Established by OMB in 2013***
- **Cybersecurity one of 14 CAP Goals**
  - ***Improve awareness of security practices, vulnerabilities, and threats to the operating environment by limiting access to only authorized users and implementing technologies and processes that reduce the risk from malicious activity***
- **Major Initiatives for FY15-17**
  - ***Information Security Continuous Monitoring (ISCM)***
  - ***Identity, Credential, and Access Management (ICAM/Strong Authentication)***
  - ***Anti-Phishing and Malware Defense (APMD)***

30-day Cybersecurity Sprint

- **Launched by U.S. CIO Tony Scott on June 12, 2015**
- **Requires Agencies to implement several immediate high priority actions to enhance cybersecurity:**
  - ***Deploying cybercrime indicators into agency anti-malware tools (e.g., scan and log analysis tools)***
  - ***Patching critical software holes based on weekly DHS security vulnerability reports***
  - ***Tightening technological controls and policies for "privileged users" or staff with high-level access to systems***
  - ***Accelerating widespread use of "multifactor authentication" or two-step ID checks***
- **Agencies to report on progress and problems complying with these procedures within 30 days**



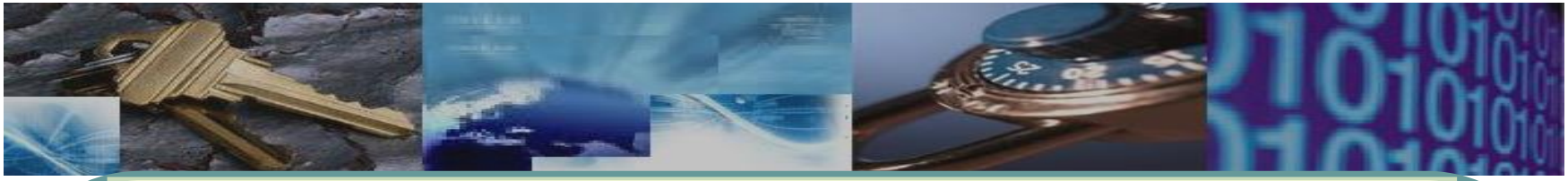
- **Current Status**
  - ***Feds still struggling to implement strong authentication for logical and physical access***

HSPD-12 Implementation Status

- **Agencies Report HSPD-12 Implementation Status on Website**
  - ***Agencies have made great progress on issuance of PIV Cards***
  - ***Many Agencies have implemented PIV-based network logon***
  - ***Very few agencies have implemented PIV-authenticated access to Agency applications***
  - ***Very few agencies have a holistic plan and approach for PIV enabling applications across the enterprise***

CAP Goal – ICAM 3Q-FY15 Status (I)

- **PIV-Usage for Unprivileged Network Users**
  - ***Goal: 85% or more***
  - ***Actual: 76% as of 8/28/15 (Civilian Agencies)***
- **PIV-Usage for Privileged Network Users**
  - ***Goal: 100%***
  - ***Actual: 73% as of 8/28/15 (Civilian Agencies)***



- **Challenges and Way Forward**
  - ***Implementation of strong authentication within Federal environments is non-trivial***

Challenges in PIV-Use – Client Side

- **User Platform Requirements**
  - ***Hardware requirements (PIV Card reader)***
  - ***Software requirements (PIV Middleware)***
- **Client Configuration Complexity**
  - ***PKI trust roots, policies***
  - ***Credential status verification***
- **User Training Challenges**
  - ***PIV use is complex and non-intuitive***
  - ***Users need explicit/detailed training (e.g., inserting the card, obtaining recipient certificates, explicitly requiring message security options)***

Challenges in PIV-Use – Application Side

- **Different Security Functions require Different Approaches**
  - ***Authentication***
  - ***Digital Signature***
  - ***Encryption (requires key recovery)***
- **Multiple types of Applications**
  - ***Network Logon***
  - ***Productivity Applications (Email, Documents)***
  - ***Enterprise Applications (Client-Server, Web-based)***
  - ***Legacy Applications***
  - ***Federated Applications (within and across Agencies)***
- **PKI Complexity**
  - ***Configurations of Trust Roots; CA Certificates***
  - ***PIV Credential Status Verification (CRL, OCSP, SCVP)***

Challenges in PIV-Use – General

- **Policy on PIV Use is high level and vague**
  - ***No real accountability for implementation***
- **Lack of Meaningful Guidance on PIV use**
  - ***Agencies struggling to meet M-11-11 targets***
  - ***Effective guidance documents need to be developed***
- **COTS Solutions are Complex and Costly**
  - ***Difficult for End Users***
  - ***Proprietary approaches***

Other Complications of PIV Use

- **Multiplicity of devices and form factors**
  - ***Mobile platforms; BYOD***
  - ***PIV Card use difficult on some***
- **Need Credentials for Devices**
  - ***Server credentials***
- **Migration to Cloud IT Environments**
  - ***Hybrid IT environment (Traditional & Cloud)***
- **PIV Derived Credentials**
  - ***PIV credentials within mobile platforms***
- **Validation of External PIV Credentials**
  - ***Complex trust paths***

Way Forward

- **Assign Agency Lead for Strong Authentication**
  - ***Form cross-functional team across Agency***
- **Categorize Applications based on Value/Impact**
  - ***Sensitivity of Information***
  - ***Criticality of Functionality/Service***
- **Classify Applications by Technology**
  - ***Develop PIV integration approach for each class***
- **Develop Policy and Timeline for PIV Integration**
  - ***Based on Application Category and Class***
- **Develop Enterprise-level Architecture for PIV Use**
  - ***Common Services***
  - ***Standardized APIs and Protocols***
- **Develop Communication and Training Materials**
  - ***Implement Outreach Plan***
- **Implement Technical Support Infrastructure**
  - ***Test Lab***
  - ***FAQs, Lessons Learned, Community Board***

Wrap Up

- **Weak authentication methods often the root cause for breaches**
- **Feds have a unique opportunity to lead in use of Strong Authentication**
- **Feds need to develop Policy and Guidance to make this happen**
- **Adoption will drive COTS vendors to develop more usable and robust authentication solutions**
- **The time to do this is NOW!**