

Interagency Advisory Board

Meeting Agenda, December 7, 2009

1. **Opening Remarks**
2. **FICAM Segment Architecture & PIV Issuance** (*Carol Bales, OMB*)
3. **ABA Working Group on Identity** (*Tom Smedinghoff*)
4. **F/ERO Repository** (*Elisa Cruz/FEMA*)
5. **Correlation of SP 800-53 rev. 3/ FIPS 201/ SP 800-63/ PIV-I/ FICAM Segment Architecture** (*Matt Scholl/Bill Macgregor, NIST*)
6. **Use of Optional Form Factor to Meet PIV-I** (*Andrew Sheedy, ActivIdentity*)
7. **Closing Remarks**

Minimum Security Requirements

FISMA Requirement

- Develop minimum information security requirements (management, operational, and technical security controls) for information and information systems in each security category defined in FIPS 199

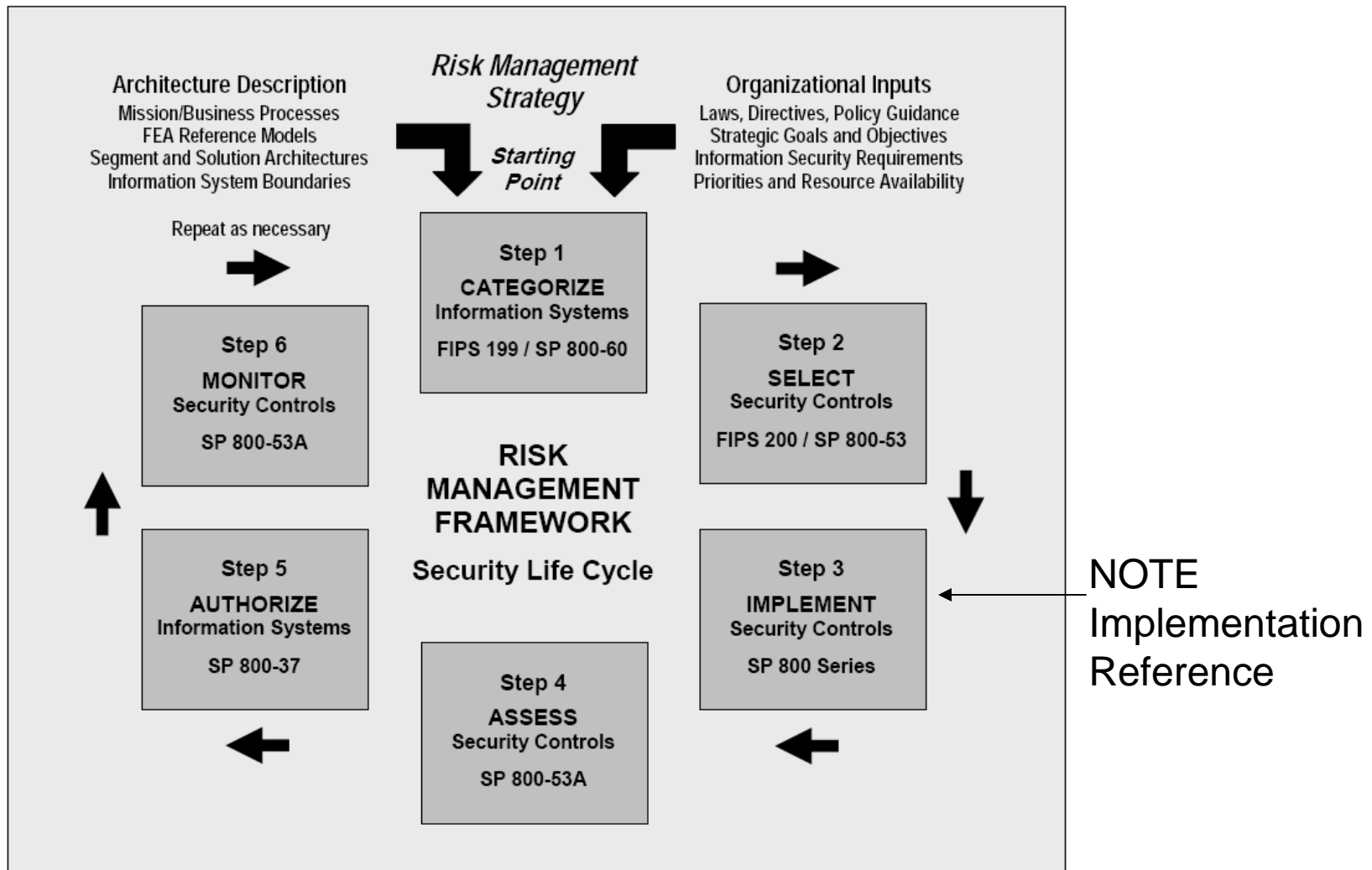
NIST Special Publication 800-53,
“Recommended Security Controls for Federal Information Systems”

Minimum Security Controls

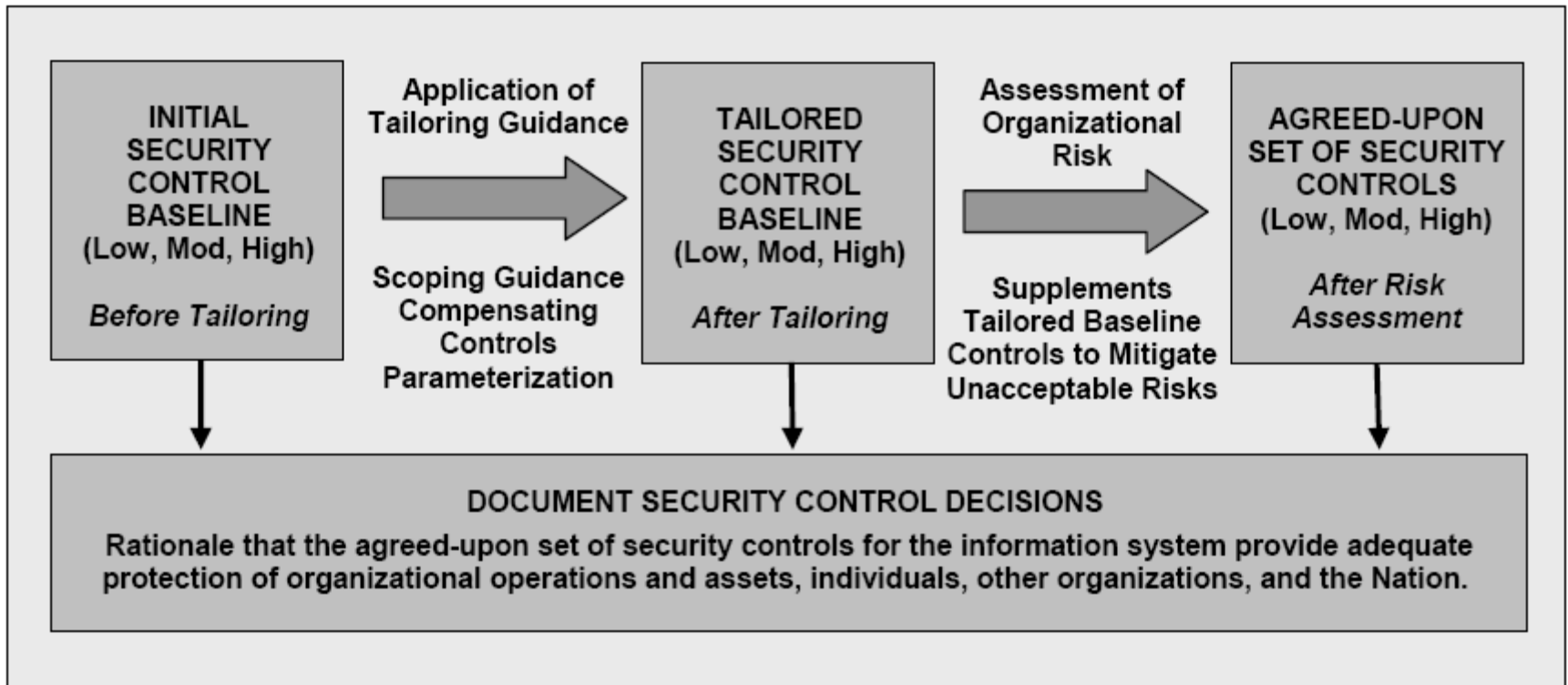
- Minimum security controls, or baseline controls, defined for low-impact, moderate-impact, and high-impact information systems—
 - Provide a ***starting point*** for organizations in their security control selection process
 - Are used in conjunction with ***scoping guidance*** that allows the baseline controls to be tailored for specific operational environments
 - Support the organization's ***risk management process***

Risk Management Framework

Core Elements for a Security Program



Security Control Selection Process



What Does Referenced in SP 800-53 Mean?

The references section³⁰ includes a list of applicable federal laws, Executive Orders, directives, policies, standards, and guidelines (e.g., OMB Circulars, FIPS, and NIST Special Publications), that are relevant to a particular security control or control enhancement.³¹ The references provide appropriate federal legislative and policy mandates as well as supporting information for the implementation of specific management, operational, or technical controls/enhancements.

³⁰ Publications listed in the *References* section of security controls refer to the most recent versions of the publications. Organizations confirm from the respective official sources of the publications (e.g., OMB, NIST, NARA), that the most recent versions are being used for organizational application.

31 The references listed in the security control references section are provided to assist organizations in applying the controls and are not intended to be inclusive or complete.

800-53 and 800-63

Referenced in Controls IA1,2,5. AC 17, MA4
and SC 17

- IA-1 IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES
- IA-2 IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users
- IA-5 AUTHENTICATOR MANAGEMENT The organization manages information system authenticators for users and devices
- AC-17 IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS) The information system uniquely identifies and authenticates non-organizational users
- MA-4 NON-LOCAL MAINTENANCE
- SC-17 PUBLIC KEY INFRASTRUCTURE CERTIFICATES

IA-1

IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES

Control: The organization develops, disseminates, and reviews/updates [*Assignment: organization defined frequency*]:

- a. A formal, documented identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
- b. Formal, documented procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls.

Supplemental Guidance: This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the identification and authentication family. **The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations,** standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The identification and authentication policy can be included as part of the general information security policy for the organization. Identification and authentication procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the identification and authentication policy. Related control: PM-9.

Control Enhancements: None.

References: FIPS Publication 201; NIST Special Publications 800-12, **800-63**, 800-73, 800-76, 800-78, 800-100.

IA-2

IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)

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

Supplemental Guidance: Organizational users include organizational employees or individuals the organization deems to have equivalent status of employees (e.g., contractors, guest researchers, individuals from allied nations). Users are uniquely identified and authenticated for all accesses other than those accesses explicitly identified and documented by the organization in AC-14.

Unique identification of individuals in group accounts (e.g., shared privilege accounts) may need to be considered for detailed accountability of activity. *Authentication of user identities is accomplished through the use of passwords, tokens, biometrics, or in the case of multifactor authentication, some combination thereof...*

IA-2

Control Enhancements:

(1) The information system uses multifactor authentication for network access to privileged accounts.

(2) The information system uses multifactor authentication for network access to non-privileged accounts.

(3) The information system uses multifactor authentication for local access to privileged accounts.

(4) The information system uses multifactor authentication for local access to non-privileged accounts.

(8) The information system uses [*Assignment: organization-defined replay-resistant authentication mechanisms*] for network access to privileged accounts.

Enhancement Supplemental Guidance: An authentication process resists replay attacks if it is impractical to achieve a successful authentication by recording and replaying a previous authentication message. Techniques used to address this include protocols that use nonces or challenges (e.g., TLS), and time synchronous or challenge-response one-time authenticators.

(9) The information system uses [*Assignment: organization-defined replay-resistant authentication mechanisms*] for network access to non-privileged accounts.

Enhancement Supplemental Guidance: An authentication process resists replay attacks if it is impractical to achieve a successful authentication by recording and replaying a previous authentication message. Techniques used to address this include protocols that use nonces or challenges (e.g., TLS), and time synchronous or challenge-response one-time authenticators.

References: HSPD 12; OMB Memorandum 04-04; FIPS Publication 201; NIST Special Publications 800-63, 800-73, 800-76, 800-78.

LOW IA-2 (1) MOD IA-2 (1) (2) (3) (8) HIGH IA-2 (1) (2) (3) (4) (8) (9)

IA-5

AUTHENTICATOR MANAGEMENT

Control: The organization manages information system authenticators for users and devices by:

- a. Verifying, as part of the initial authenticator distribution, the identity of the individual and/or device receiving the authenticator;
- b. Establishing initial authenticator content for authenticators defined by the organization;
- c. Ensuring that authenticators have sufficient strength of mechanism for their intended use;
- d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators;
- e. Changing default content of authenticators upon information system installation;
- f. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators (if appropriate);
- g. Changing/refreshing authenticators [*Assignment: organization-defined time period by authenticator type*];
- h. Protecting authenticator content from unauthorized disclosure and modification; and
- i. Requiring users to take, and having devices implement, specific measures to safeguard Authenticators

IA-5

Control Enhancements:

(1) The information system, for password-based authentication:

(a) Enforces minimum password complexity of [Assignment: organization-defined requirements for case sensitivity, number of characters, mix of upper-case letters, lower-case letters, numbers, and special characters, including minimum requirements for each type];

(b) Enforces at least a [Assignment: organization-defined number of changed characters] when new passwords are created;

(c) Encrypts passwords in storage and in transmission;

(d) Enforces password minimum and maximum lifetime restrictions of [Assignment: organization defined numbers for lifetime minimum, lifetime maximum]; and

(e) Prohibits password reuse for [Assignment: organization-defined number] generations.

Enhancement Supplemental Guidance: This control enhancement is intended primarily for environments where passwords are used as a single factor to authenticate users, or in a similar manner along with one or more additional authenticators. The enhancement generally does *not* apply to situations where passwords are used to unlock hardware authenticators. The implementation of such password mechanisms may not meet all of the requirements in the enhancement.

(2) The information system, for PKI-based authentication:

(a) Validates certificates by constructing a certification path with status information to an accepted trust anchor;

(b) Enforces authorized access to the corresponding private key; and

(c) Maps the authenticated identity to the user account.

Enhancement Supplemental Guidance: Status information for certification paths includes, for example, certificate revocation lists or online certificate status protocol responses.

(3) The organization requires that the registration process to receive [Assignment: organization defined types of and/or specific authenticators] be carried out in person before a designated registration authority with authorization by a designated organizational official (e.g., a supervisor).

AC-17

REMOTE ACCESS

Control: The organization:

- a. Documents allowed methods of remote access to the information system;
- b. Establishes usage restrictions and implementation guidance for each allowed remote access method;
- c. Monitors for unauthorized remote access to the information system;
- d. Authorizes remote access to the information system prior to connection; and
- e. Enforces requirements for remote connections to the information system.

MA-4

NON-LOCAL MAINTENANCE

Control: The organization:

- a. Authorizes, monitors, and controls non-local maintenance and diagnostic activities;
- b. Allows the use of non-local maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the information system;
- c. Employs strong identification and authentication techniques in the establishment of non-local maintenance and diagnostic sessions;
- d. Maintains records for non-local maintenance and diagnostic activities; and
- e. Terminates all sessions and network connections when non-local maintenance is completed.

SC-17

PUBLIC KEY INFRASTRUCTURE CERTIFICATES

Control: The organization issues public key certificates under an appropriate certificate policy or obtains public key certificates under an appropriate certificate policy from an approved service provider.

Supplemental Guidance: For user certificates, each organization attains certificates from an approved, shared service provider, as required by OMB policy. For federal agencies operating a legacy public key infrastructure cross-certified with the Federal Bridge Certification Authority at medium assurance or higher, this Certification Authority will suffice. This control focuses on certificates with a visibility external to the information system and does not include certificates related to internal system operations, for example, application-specific time services.

Control Enhancements: None.

References: OMB Memorandum 05-24; NIST Special Publications 800-32, 800-63.

Some Definitions Used

Multifactor Authentication

Authentication using two or more factors to achieve authentication.

Factors include: (i) something you know (e.g. password/PIN); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric). [SP 800-53]