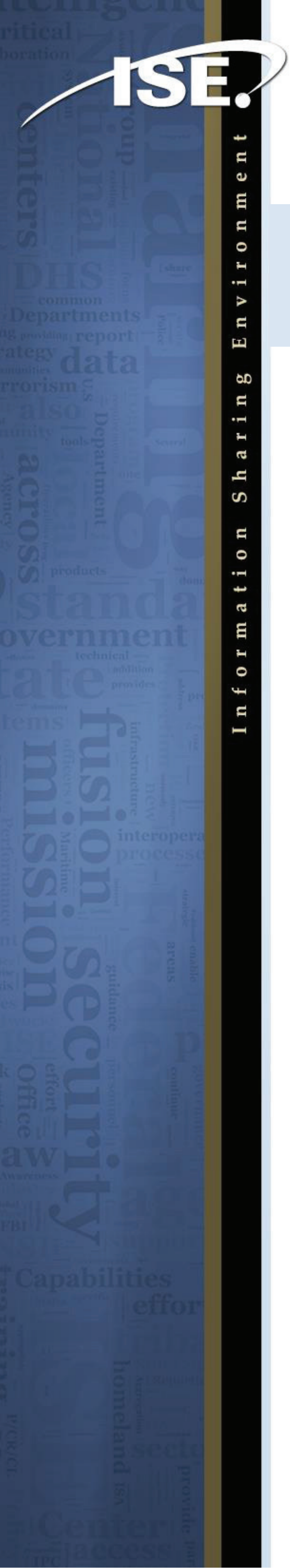

INTRODUCTION TO ICAM PRINCIPLES

IDENTITY, CREDENTIAL, AND ACCESS MANAGEMENT

ICAM—**IDENTITY, CREDENTIAL, AND ACCESS MANAGEMENT**—is the set of security disciplines that allows an organization to enable the right individual to access the right resource at the right time for the right reason.

We perform ICAM-related functions dozens of times per day, often without realizing it: when we unlock our cars, swipe into and out of the subway/metrorail, check our email, and withdraw cash at an ATM. Can you imagine if anyone could withdraw cash from your account? Or if anyone could start your car?

1 IDENTITY MANAGEMENT

Identity Management is the set of practices that allow an organization to establish, maintain, and terminate identities.

An **IDENTITY** is the set of characteristics (also called "attributes") that describe an individual **within a given context**:

- Your identity within the context of the Department of Motor Vehicles (DMV) is different from your identity within the context of your bank.
- Similarly, a person who is both a government contractor and an Army Reservist will have two identities, one in each context. These identities are often called "personas."

Identities change and evolve over time (you may get a promotion, change your hair color, or receive additional training) and may be terminated (you may turn in your driver's license when you move to another state), but **identities do not expire**.

IDENTITY PROOFING is the process by which an identity is first established. This process can be simple or complicated, depending on the Level of Assurance (strength) that is required of the identity:

- The process for a frequent shopper program at the local grocery store is weak.
- The processes required by the DMV is stronger, typically requiring multiple forms of evidence, such as leases, mortgages, and utility bills.
- The process required by the Federal Government is stronger still.

An **IDENTIFIER** is a unique attribute that can be used to locate a specific identity within its context:

While the DMV may issue many driver's licenses bearing the same name (there is more than one John Smith in the state), each will have a different driver's license number.

2 CREDENTIAL MANAGEMENT

Credential Management is the set of practices that an organization uses to issue, track, update, and revoke credentials for **identities within their context**.

A **CREDENTIAL** is authoritative evidence of an individual's claimed identity. Credentials come in many types, from physical papers and cards (such as a passport or ATM card) to electronic items (such as a password or digital certificate), and often incorporate anti-tamper features.

All credentials, no matter what type, associate an identity with an individual (typically via an identifier) and identify the organization that issued it:

- Your driver's license includes a license number, your name, and a state seal.
- An ATM card includes a card number, your name, and a corporate symbol.

Some credentials indicate authorizations granted to the identity by the issuing organization. For example, a driver's license includes the authorization to drive a car.

Unlike identities, **credentials generally expire**. If an identity continues past the expiration date of the credential, a new credential is issued:

- Your driver's license expires after so many years and you receive a new one.
- Your ATM card expires after so many years and you receive a new one.

A credential that is lost or compromised before it expires may be revoked by the organization that issued it.

Credentials can incorporate something you know (such as a password or PIN), something you have (such as a card), or something you are (such as a fingerprint or iris). Some credentials incorporate more than one, and are referred to as two-factor or multi-factor.

As with identity proofing, credentials have different Levels of Assurance depending on the strength required. The credential for accessing your bank account is likely stronger than the credential for accessing your health club.

3 ACCESS MANAGEMENT

Access Management is the set of practices that enables only those permitted the ability to perform an action on a particular resource.

POLICY MANAGEMENT is the process by which laws, regulations, rules, and organizational/corporate access policies are put into effect. These policies may be extremely simple, extremely complicated, or anywhere in between.

For example:

- "Grant access to anyone who knows the secret handshake."
- "Grant access to anyone on this list of people."
- "Grant access to anyone in Human Resources."
- "Grant access to anyone who is a federal employee, GS-12 or higher, cleared Top Secret, trained in first aid, and certified as a project manager."

AUTHORIZATION is the adjudication of requests. Please see the section on Authorization on the reverse side of this page for more details.

4 BRING YOUR OWN IDENTITY

Bring your own identity is the ability to use an identity and credential from one context in another.

> For example, a bar does not conduct an Identity Proofing process to establish your identity and issue you a credential within the context of that specific bar. Rather, the bar accepts your driver's license even though it is from a different context.

This same idea is being applied in the electronic space as well: many websites now accept external identities (such as Facebook®, Twitter®, LinkedIn®, Google+® or Amazon®) for access, rather than having to obtain a new credential (such as a login name and password) for each website. These websites accept the external identity and credential, even though they are from a different context.

5 AUTHENTICATION

Authentication is the process by which a claimed identity is confirmed, generally through the use of a credential:

- When going through airport security, you present your driver's license, confirming your identity as the ticketed passenger.
- When you attempt to withdraw cash at an ATM, you present your ATM card and enter your personal identification number (PIN), confirming your identity as the account holder.

Authentication is generally a two-step process:

Step 1. Authenticate the credential itself:

- Was the credential issued by a trusted organization?
- Has the credential expired?
- Has the credential been revoked, voided, or tampered?

Step 2. Ensure that the individual the credential was issued to is the same individual that is presenting it:

- Does the photo and height/weight on the driver's license match the person who presented it?
- Does the person know the PIN for the ATM card that was presented?

Authentication is how you **confirm who you are**. Identity proofing is performed to **establish** an identity, whereas authentication is performed to **use** an identity.

6 AUTHORIZATION

Authorization is the decision portion of Access Management: the process by which a request to perform an action on a resource is decided, typically based on a policy. The range of possible requests is very broad:

- A request to read a certain document.
- A request to receive a benefit.
- A request to enter a facility or location.

In some cases, it is necessary to perform authentication in order to perform authorization:

> When you present your driver's license at a bar, you are simultaneously authenticating (the bartender ensures the photo on the license matches the person) and authorizing (the bartender ensures you are old enough).

In other cases, authorization can occur without authentication:

> When you unlock your car, the car is authorizing you without knowing who is holding your keys. If you give your keys to a friend, he or she is just as able to unlock your car as you are, and the car does not know the difference.

Authorization is how your **request for a resource is decided**.

7 FEDERATION

Federation is the ability of one organization to accept another organization's work. Federation is based on **inter-organizational trust**. The trusting organization has to be comfortable that the trusted organization has similar policies, and that those policies are being followed:

- A credential issued by your local library will not likely be trusted by the security staff at the White House.
- A credential issued by your bank may be trusted by your health club.

Federation can occur at different points within ICAM. Examples include:

An organization can accept credentials issued by another organization, but still authenticate and authorize the individual locally:

> A passport issued by the U.S. Department of State is accepted as a valid credential by a foreign country, but that country's immigration office still authenticates the holder and requires a visa (authorization).

An organization can accept specific characteristics (attributes) describing an individual from another organization:

> Your bank will request your credit score from one of the credit bureaus, rather than maintaining that information itself.

An organization can accept an authorization decision from another organization:

> A driver's license authorizing you to drive in one state is accepted by another.