



# ISOAG Meeting August 31, 2016

Welcome to CESC



# ISOAG August 31, 2016 Agenda

- |   |  |
|---|--|
| <b>I. Welcome &amp; Opening Remarks</b>   | <b>Mike Watson, VITA</b>                                 |
| <b>II. How Implementing Archer Can Provide In Automating Risk &amp; Compliance Related Activities For VA Agencies</b> | <b>Alyson Intihar, RSA<br/>&amp;<br/>Dan Minter, RSA</b> |
| <b>III. NSTIC Transition Plan From Startup To Operational To Ultimate Shutdown</b>                                    | <b>Paul Grassi, NSTIC</b>                                |
| <b>IV. Upcoming Events</b>  | <b>Mike Watson, VITA</b>                                 |
| <b>V. Partnership Update</b>  | <b>Northrop Grumman</b>                                  |



# Welcome and Opening Remarks

**Michael Watson**

**August 31, 2016**



**Dan Minter, RSA  
&  
Alyson Intihar, RSA**

**August 31, 2016**



# GRC FOR VIRGINIA AGENCIES

ISOAG AUGUST 31<sup>ST</sup>, 2016

DAN MINTER – SENIOR SALES ENGINEER

ALYSON INTIHAR – ARCHER ACCOUNT MANAGER



# **INSPIRE EVERYONE TO OWN RISK**



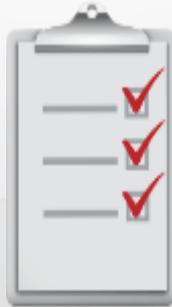
# Governance, Risk, & Compliance Today

Companies are focusing their budgets and time toward compliance, while managing and embracing risk is secondary

Outdated Reporting



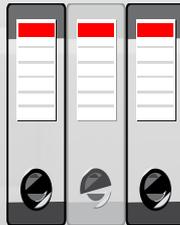
Manual Processes



Lack of Ownership



Information Silos



Inconsistent Controls



Limited Risk Visibility



# Risk Is Multi-Dimensional

Empower a common risk conversation



- Broadest suite of integrated solutions
- Rapid implementation
- Business context

'Most companies do not have a consistent way of assessing risk across the enterprise. 20% of companies say there is no process to develop and aggregate a risk profile and a further 38% rely on a self-assessment by the business units. Almost half profess difficulties in understanding their enterprise-wide risk exposure.'

- *Global Risk Survey: Expectations of Risk Management Outpacing Capabilities—It's Time for Action*, KPMG, 2013.

# Business Continuity Risk Assessment *...through the power of GRC*

# How does this apply to me?

NIST.SP.800-53Ar4 CP-9 a-1, CP-9 b-1, CP-9 c-1

Information Security assessment procedures call for the following evidence to be present in your control environment:

*defines a frequency, consistent with recovery time objectives and recovery point objectives as specified in the information system contingency plan, to conduct backups of user-level information contained in the information system;*

NIST.SP.800-53Ar4 CP-1, CP-2

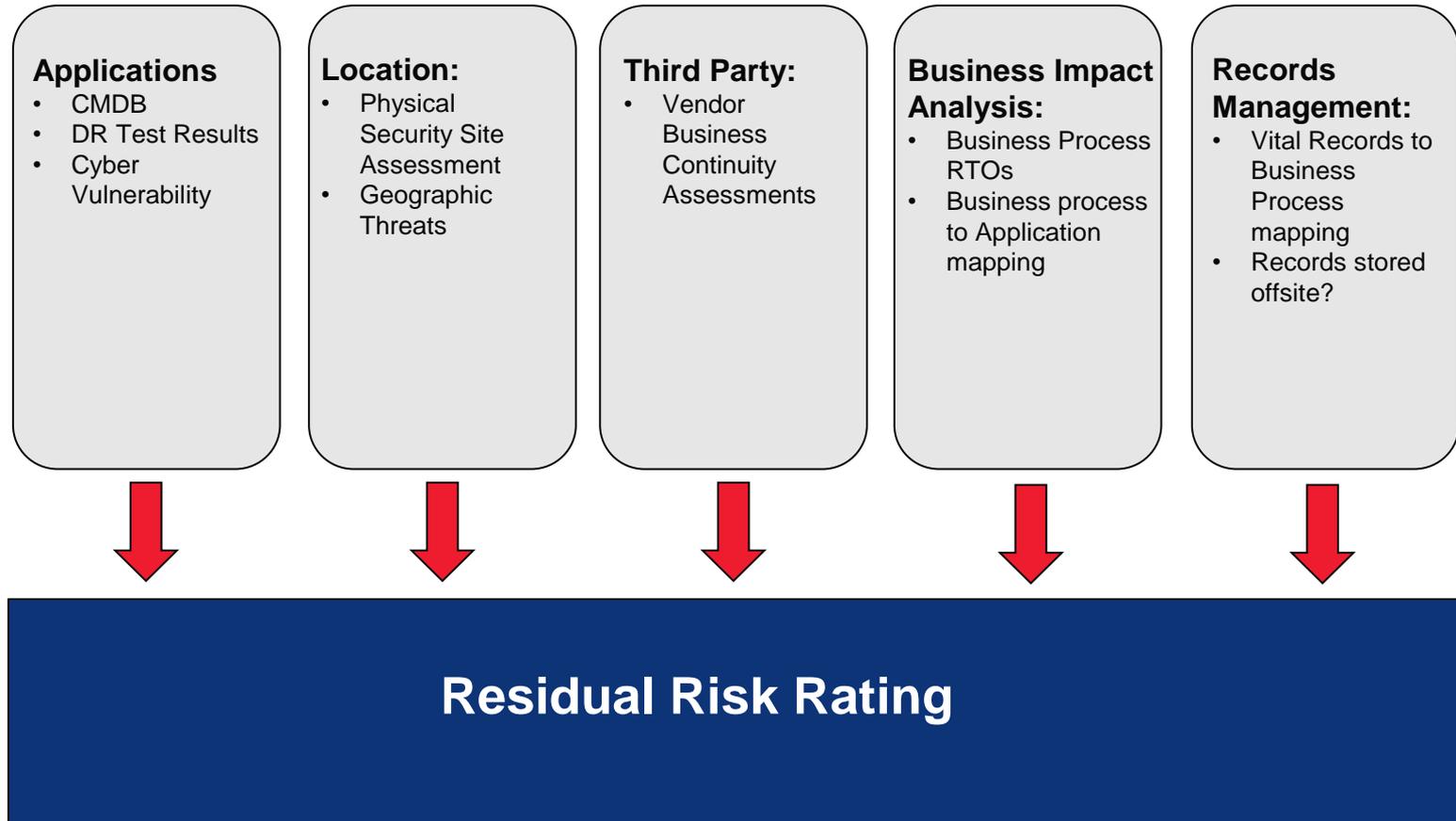
contingency planning security control, may be considered a hybrid control by the organization if there is a contingency plan developed by the organization for all organizational information systems. Following up on the initial contingency plan, information system owners are expected to adjust or tailor the contingency plan as necessary, when there are specific aspects of the plan that need to be defined for the particular system where the control is employed. For each

# ISO 22301 touches it all...



# What data sources do you need?

The answer is the key to unlocking the true power of an integrated GRC program



# Application BC Risk

## ▶ Inputs to BC Risk:

- List of all in scope applications from the most recent Disaster Recovery exercise
- Did the application beat the RTOs defined by the business, the customers, or IT?
- Do any of these applications have known logical vulnerabilities that are pending resolution?

## ▶ Resulting Risk Level:

- If RTO not met, then risk = High
- If RTO met and unresolved vulnerability exists, then risk = Medium
- If RTO met and no known vulnerabilities, then risk = Low

# Business Continuity Capability Risk

- ▶ **RTO (inherent risk) of business functions per location from BIA**
- ▶ **Associated recovery strategies from BIA and whether they can beat RTO**
  - RTO under 4 hours = Transfer work strategy
  - RTO 4 – 12 hours = Workplace recovery site
  - RTO 12 hours and above = Work from home
- ▶ **Vital records stored on-site?**

## Third Party Risk

- ▶ Does the 3rd Party have a High, Medium, or Low Business Continuity risk as determined by Third Party Oversight?

Values (High, Medium, Low) are brought into the Residual Risk (as is)

- ▶ Optional: factor in the overall Third Party Oversight risk rating for the vendor because it will include assessment data on more than just Business Continuity readiness

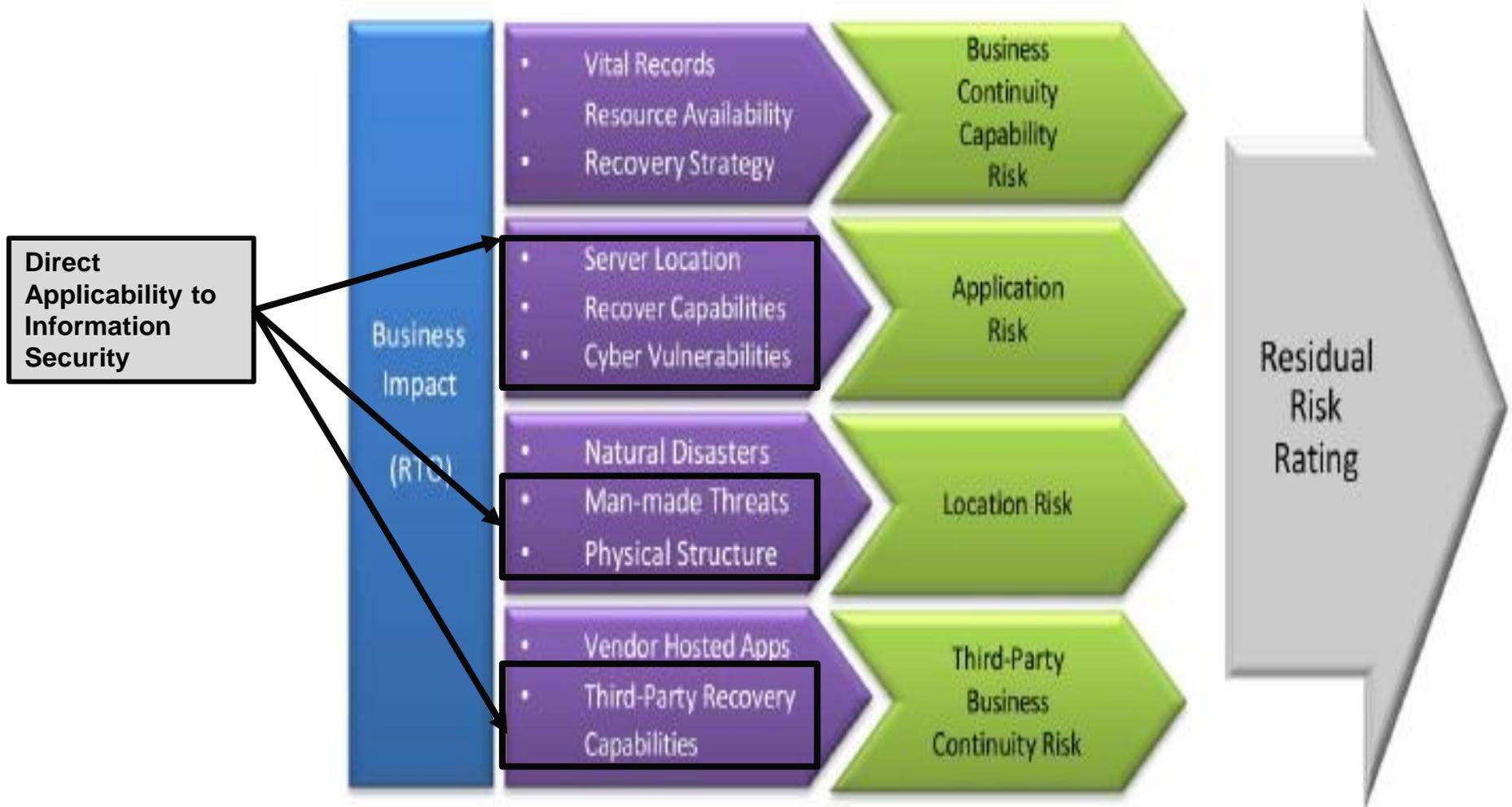
# Location Risk

Geographic Threats and likelihood of BC event as a result

Physical Security Site Assessment (specific to your organization)

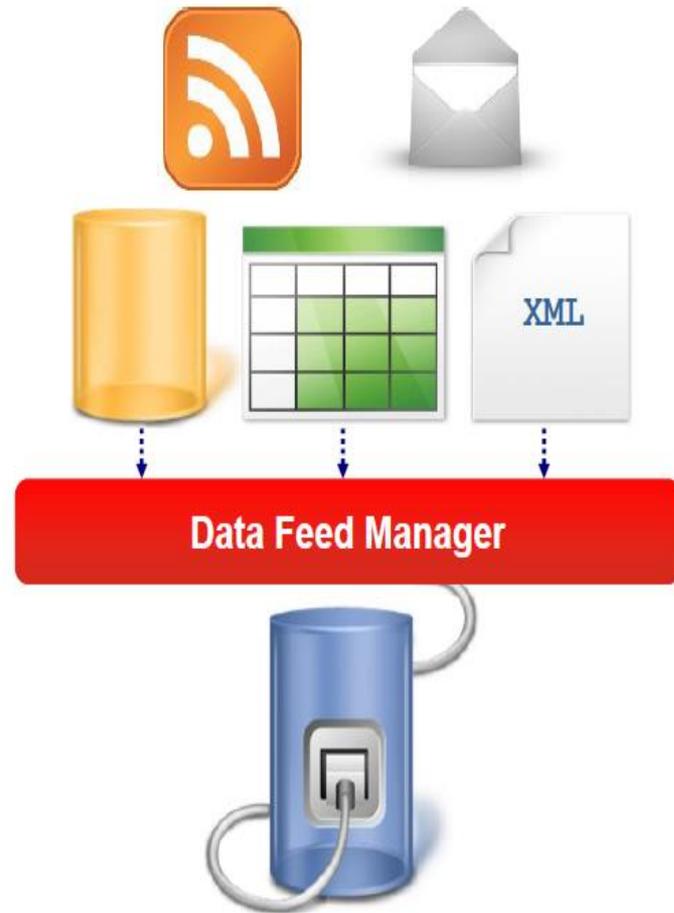


# BCM Risk Assessment

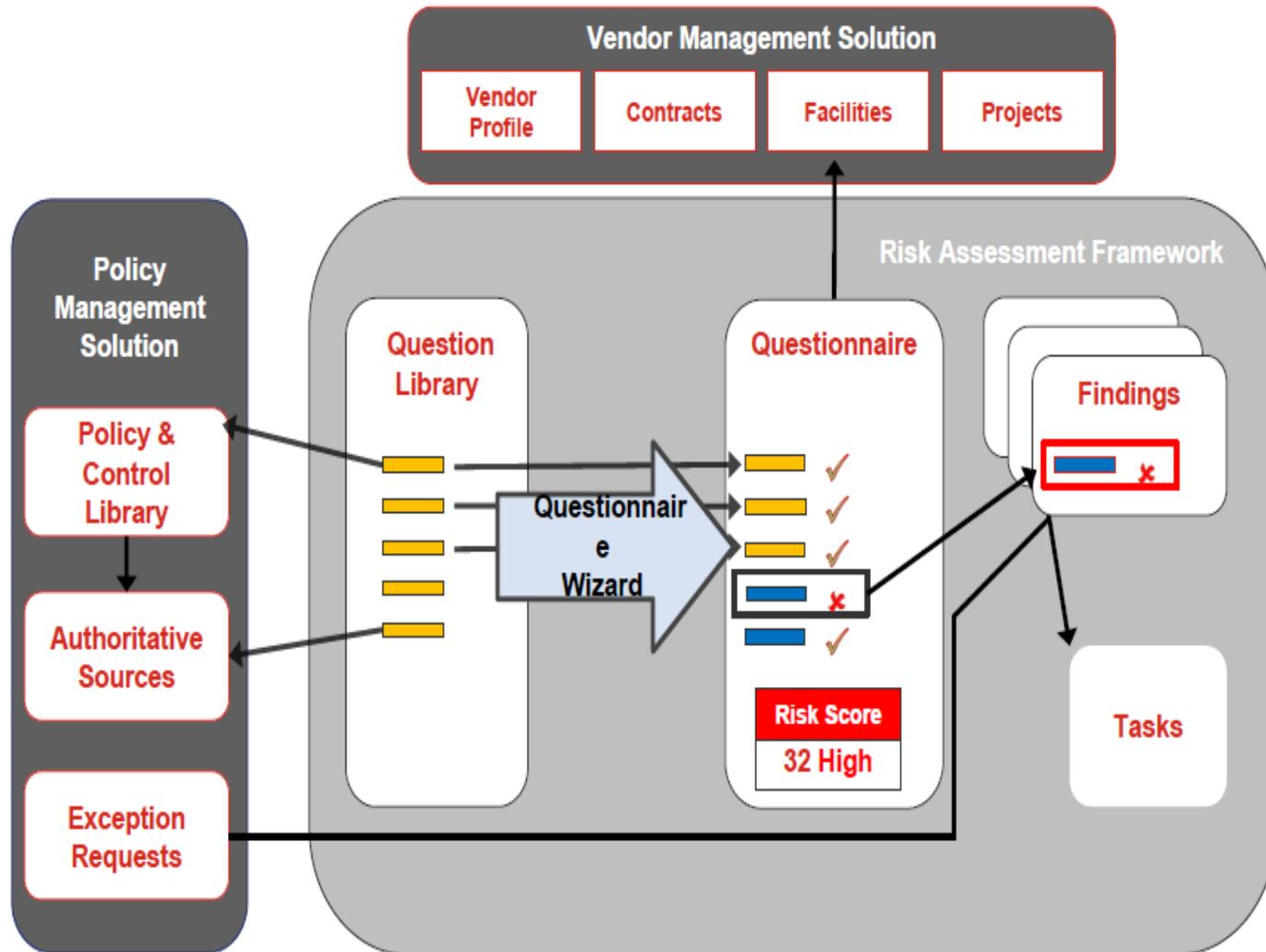


# Data Feed Manager – This is how it gets done!

- ▶ Extracts information from a variety of sources in a variety of formats
- ▶ Transform and filter the data as necessary
- ▶ Set an automatic schedule that best fits the business needs



# Archer Risk Framework



# Return on Investment

## Category

## Benefits

### Third-Party Oversight

- The model now incorporates vendor risk into the residual risk calculation.
- Vendor risk data is sourced directly from the Third party Oversight organization.

### Cybersecurity

- The model now incorporates known cyber vulnerabilities into the residual risk calculation.
- Cyber risk data is sourced directly from the Security Architecture organization.

### Location Risk

- The model now incorporates a data-drive approach to location-specific risks such as natural disasters and weather events.
- Data sources include the National Weather Service, USGS, and Physical Security site assessments.

### Automation

- Moving away from a manual process reduces the potential for user error, and reduces the manual burden to generate the Risk Assessment.
- Automated reporting increases visibility of Business Continuity risks stakeholders and eases incorporation of these risks into the Issue Management process.
- Use of the Archer platform increases cohesion and data sharing between risk management groups across the enterprise.
- Removed dependency on external consultants and transferred process

**RSA<sup>®</sup>**

**EMC<sup>2</sup>**

EMC, RSA, the EMC logo and the RSA logo are trademarks of EMC Corporation in the U.S. and other countries.

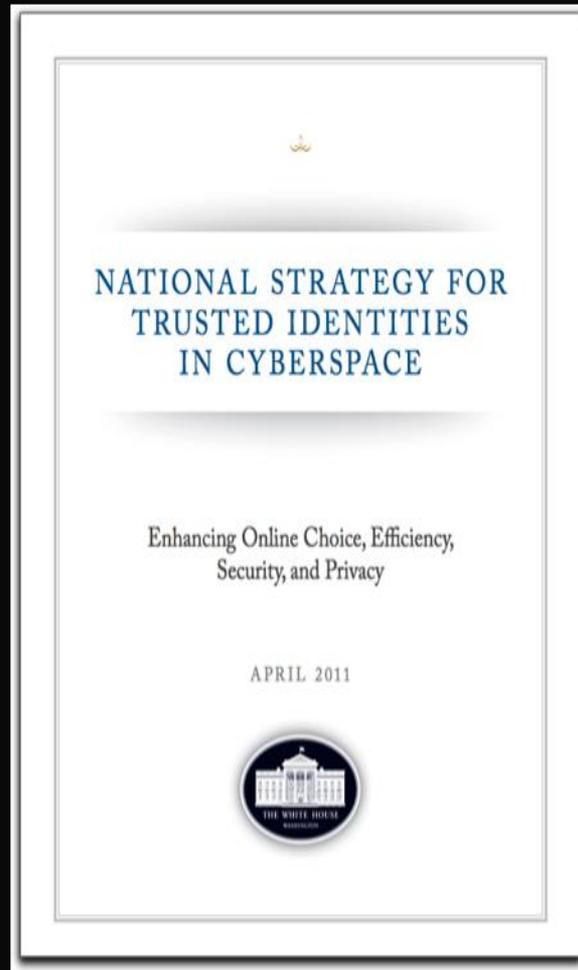


*Virginia Information Technologies Agency*

# Paul Grassi, NIST



# THE NSTIC UPDATE



July 14<sup>th</sup>, 2016

# It's 2011.

Most American adults (79%) use the Internet.

The average user needs 10 different passwords daily.

It's a year of unprecedented data breaches.

It's the year Google releases two-factor authentication.

**The U.S. government releases an ambitious strategy  
to improve digital identity and online interactions.**

# THE GOAL:

enhance choice,  
efficiency, security,  
and privacy online

by advancing a marketplace of identity solutions



privacy  
enhancing &  
voluntary



secure &  
resilient



interoperable



cost effective &  
easy-to-use

# THE MODEL: part 1

## **bring together businesses & industry leaders**

IDESG: independent organization; ~300 members;  
IDEF released October 2015; IDEF Registry went live June 2016

---

## **set the marketplace in motion**

24 pilots: 150+ partners; 26 states and DC  
5.9 million impacted; 12 industries; 10 MFA solutions

---

## **establish government as an early adopter**

NIST



yubico



gemalto  
security to be free

IDESG

Ohio DAS  
Service · Support · Solutions



hydrantid

CEDARS-SINAI



Daon



INTERNET<sup>2</sup>



HealthIDx

ID.me



It's 2016.

Implementation shows  
signs of success

we are here(ish)



# Six new pilots

**yubico**

enabling secure online access to educational resources for students in Wisconsin and to state services for residents of Colorado with FIDO Alliance U2F-based YubiKeys

**Ohio DAS**  
Service · Support · Solutions

implementing a range of identity-related capabilities including multi-factor authentication to stronger identity proofing, for three state services

**gemalto**  
security to be free

working with departments of motor vehicles to issue digital driver licenses to residents of Idaho, Maryland, Washington, D.C., and Colorado

**CEDARS-SINAI**

implementing a federated identity, single sign on, multi-factor authentication solution across distinct healthcare systems for patients and providers



**ID.me**

working with the City of Austin, Texas, to develop a city level blueprint for increased trust between participants in the sharing economy and the State of Maine to implement a federated identity model for applications

**FLORIDA**  
DEPARTMENT OF REVENUE

implementing a federated identity, single sign on, multi-factor authentication solution across distinct healthcare systems for patients and providers

# mission not yet accomplished.

we are here(ish)



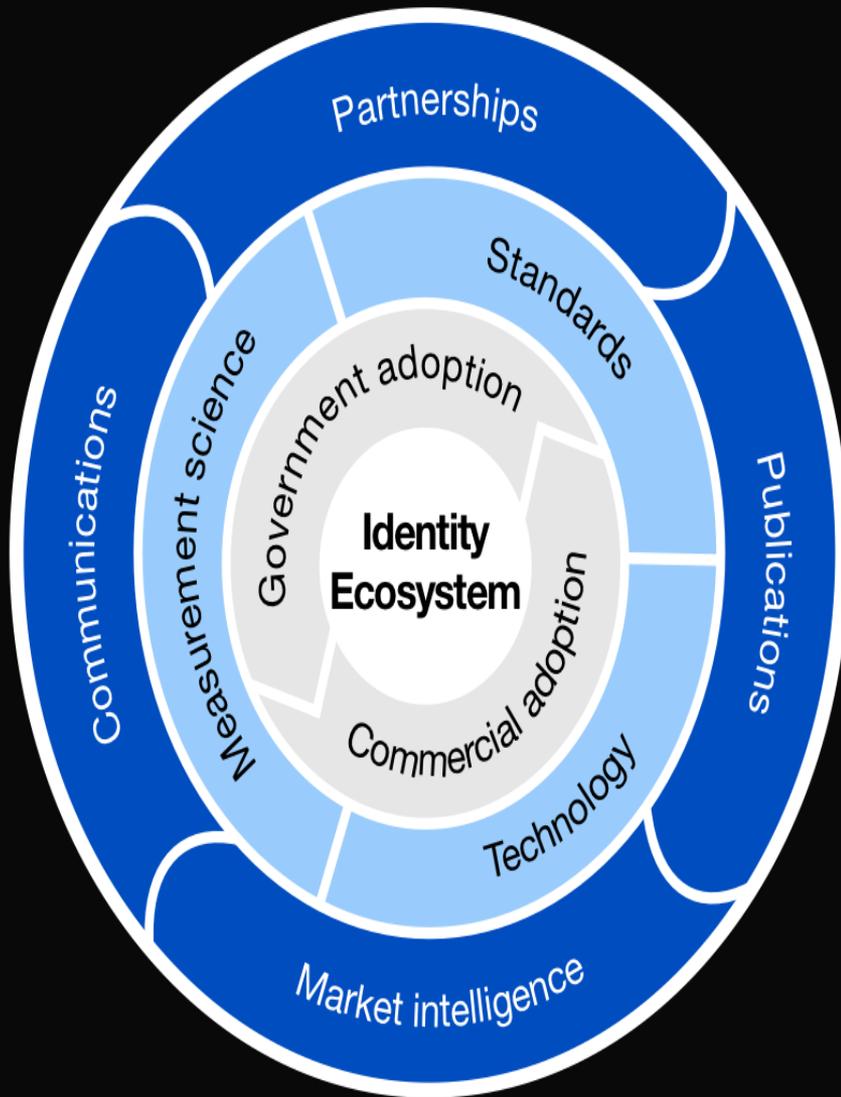
[insert declaration  
of success here]



# we must accelerate adoption



# THE MODEL: part 2



evolve & sustain  
the identity ecosystem

# smarter engagement to strengthen the market

more technical deep dives  
more high level, public awareness

## Communications



foster a more coherent community  
establish global reach

## Partnerships



Market intelligence  
track and share market trajectory  
strategically direct investment



Publications  
seek US, global, and industry alignment  
invest in what market won't support

# be risk based. be agile. be global.

OIDF/HEART

IDESG

privacy risk management

OIDF/iGov

800-63/GPG alignment

pilots → challenges

FIDO

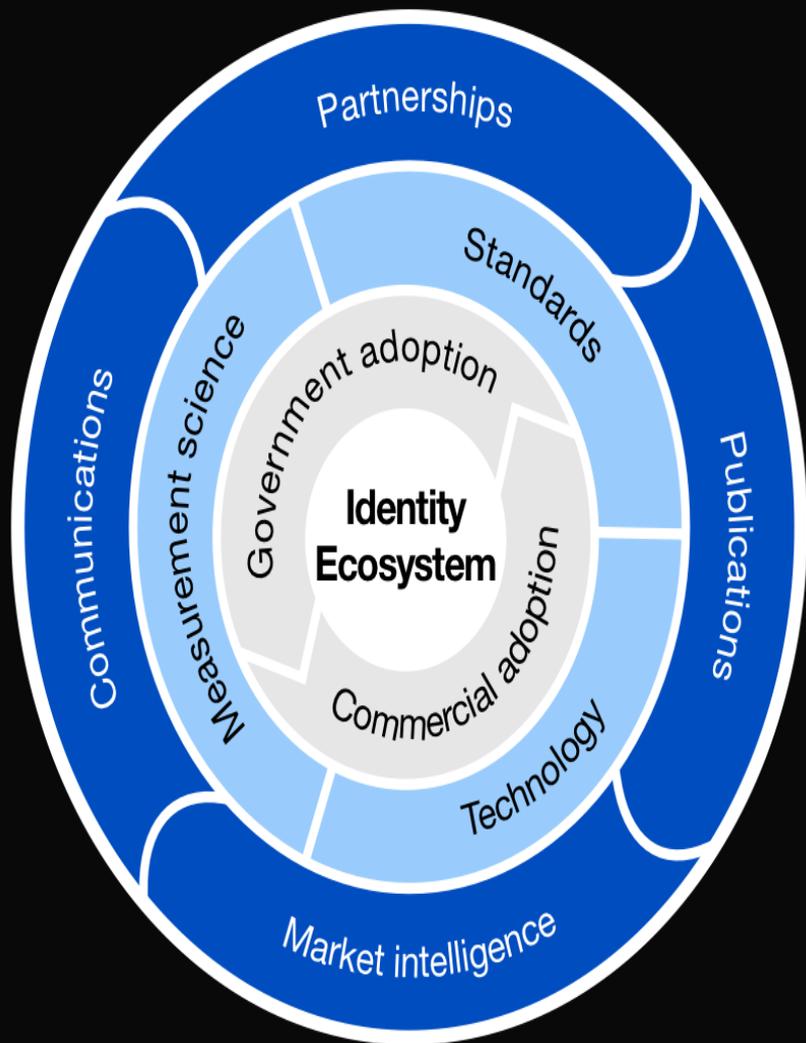
international pilots

U.S. Mobile Connect

strength of IdM frameworks

TFS reboot

IDEF: baseline → higher LOA



“gettin’ NISTy with it”

– unnamed NIST official

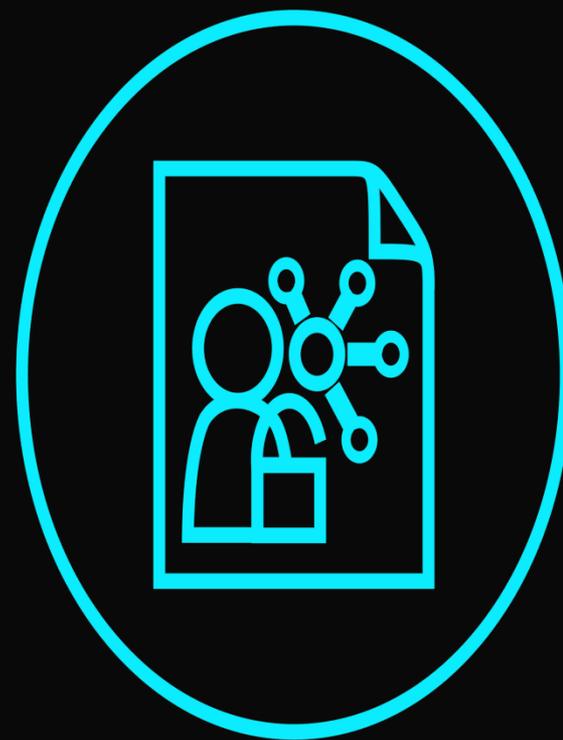
# standards, technology, & measurement science



# Updating federal guidance (more on this later)

for example: collecting  
community input on NIST  
Special Publication 800-63-3:  
*Digital Authentication Guideline*

**Goal: guidance that makes  
room for innovation**



# Exploring how to best compare identity solutions to one another



identity proofing  
credentials  
attributes

# iGov: profile the right way

Enabling people to prove  
their identities online and  
share information with  
government services  
across the globe



be risk based. be agile. be global.

# It's 2021.

2016



success declared



# Draft Special Publication 800-63-3

## Digital Authentication Guideline *(formerly known as Electronic Authentication Guideline)*



**SP 800-63-3**  
Digital Authentication  
Guideline



**SP 800-63A**  
Identity Proofing &  
Enrollment



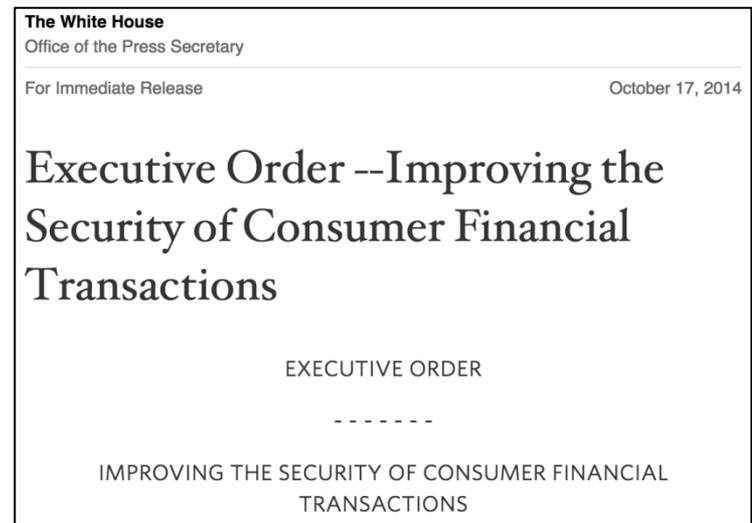
**SP 800-63B**  
Authentication &  
Lifecycle Management



**SP 800-63C**  
Federation &  
Assertions

# Why the update?

- Implement Executive Order 13681: *Improving the Security of Consumer Financial Transactions*
- Align with market and promote (adapt to) innovation
- Simplify and provide clearer guidance
- International alignment

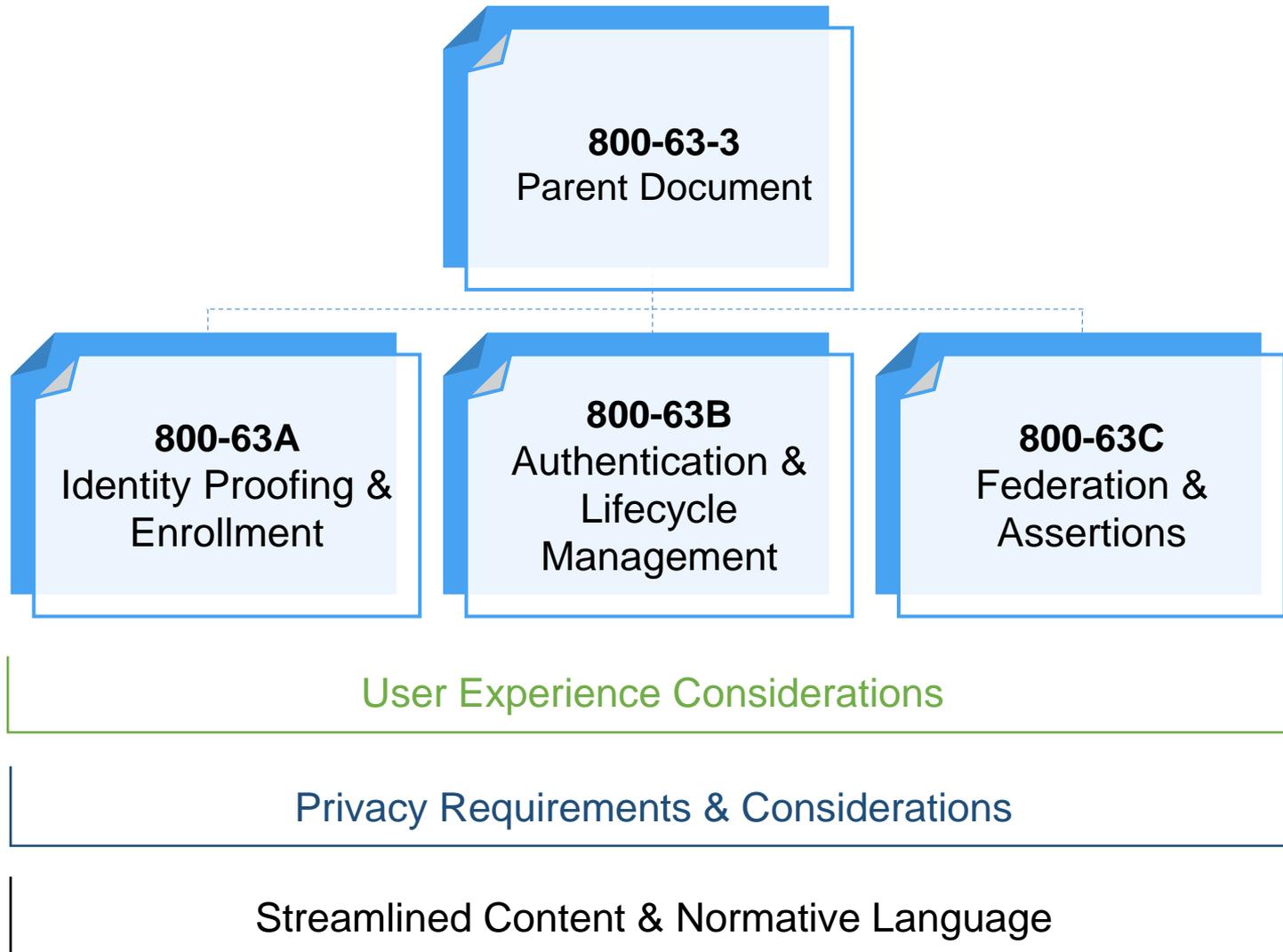




**SP 800-63-3**

**Digital Authentication Guideline**

# Making 800-63 More Accessible

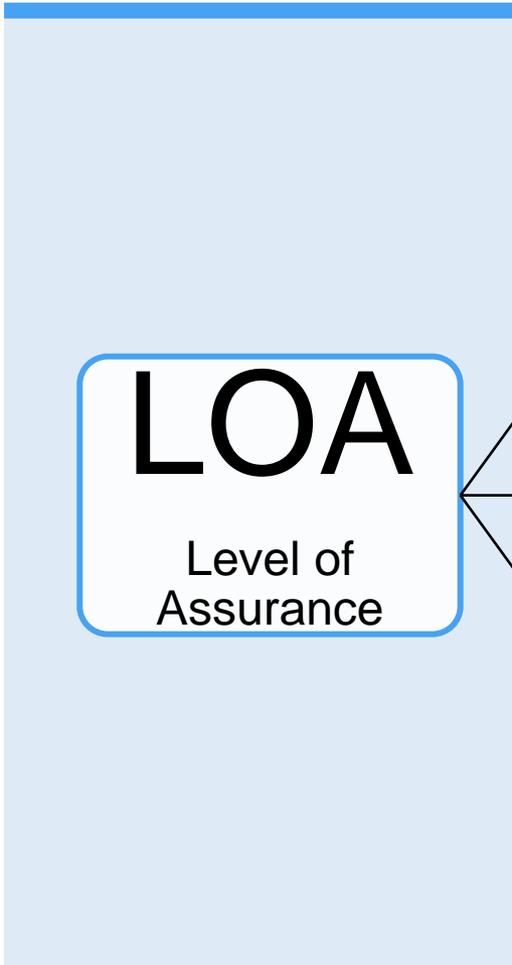


# Reference to Previous Versions of 800-63

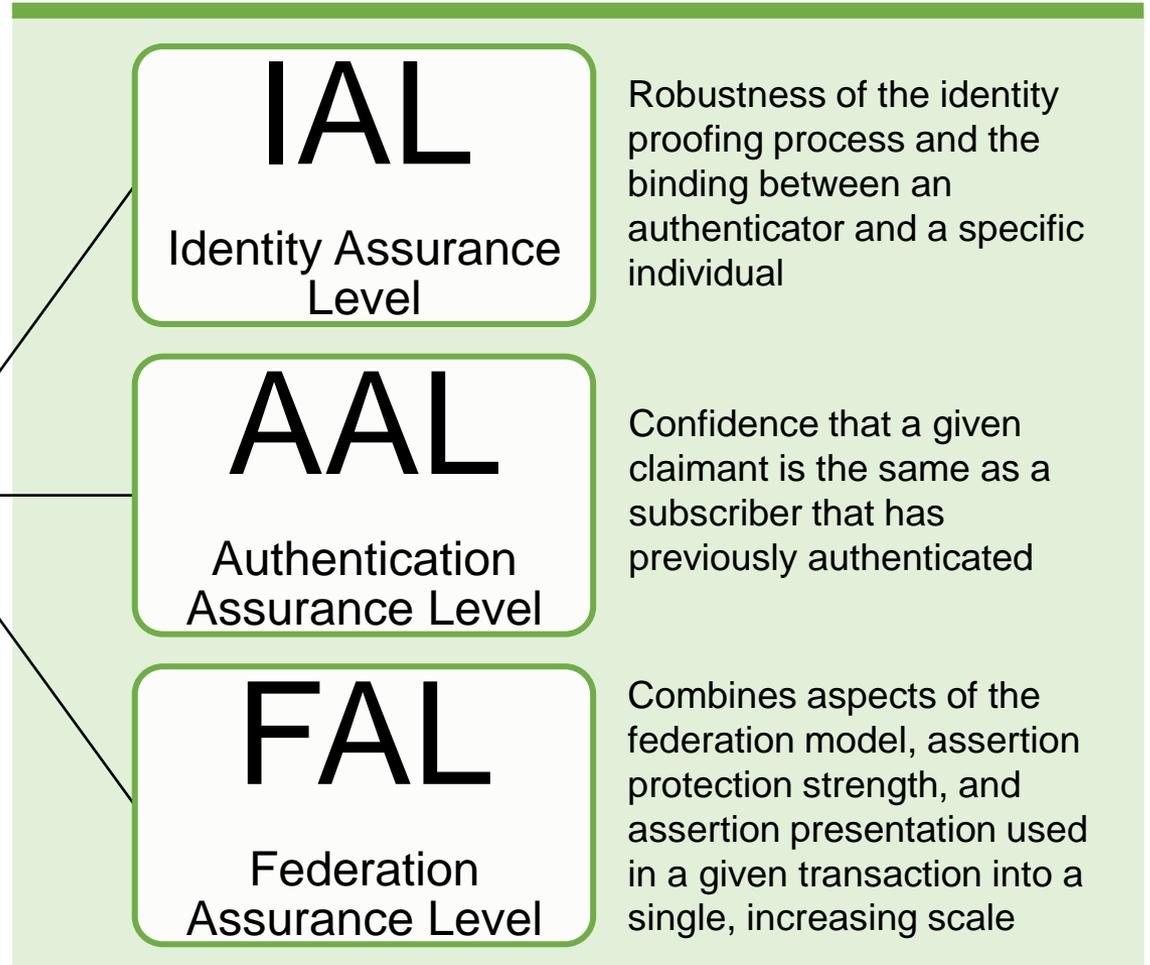
<b>800-63-2</b>	<b>New</b>
Sections 1 – 4	800-63-3
Section 5	800-63A
Sections 6 – 8	800-63B
Section 9	800-63C

# New Model

Old



New



# Identity Assurance Levels (IALs)

Refers to the robustness of the identity proofing process and the binding between an authenticator and a specific individual

IAL	Description
1	Self-asserted attribute(s) – 0 to n attributes
2	Remotely identity proofed
3	In-person identity proofed

# Authenticator Assurance Levels (AALs)

Describes the robustness of confidence that a given claimant is the same as a subscriber that has previously authenticated

AAL	Description
1	Single-factor authentication
2	Two-factor authentication
3	Two-factor authentication with hardware token

# Federation Assurance Levels (FALs)

Combines aspects of the federation model, assertion protection strength, and assertion presentation used in a given transaction into a single, increasing scale

FAL	Direct Presentation Requirement	Indirect Presentation Requirement
1	Bearer assertion, asymmetrically signed by CSP	Bearer assertion, asymmetrically signed by CSP
2	Bearer assertion, asymmetrically signed by CSP	Bearer assertion, asymmetrically signed by CSP and encrypted to RP
3	Bearer assertion, asymmetrically signed by CSP and encrypted to RP	Bearer assertion, asymmetrically signed by CSP and encrypted to RP
4	Holder of key assertion, asymmetrically signed by CSP and encrypted to RP	Holder of key assertion, asymmetrically signed by CSP and encrypted to RP

# If you love M-04-04...

<b>M-04-04 Assurance</b>	<b>IAL</b>	<b>AAL</b>	<b>FAL</b>
1	1	1	1
2	2	2 or 3	2
3	2	2 or 3	2
4	3	3	4

# ...but, digital services today

M-04-04 Assurance	IAL	AAL	FAL
1	1	1, 2 or 3	1, 2, 3, or 4
2	1 or 2	2 or 3	2, 3, or 4
3	1 or 2	2 or 3	2, 3, or 4
4	1, 2 or 3	3	3 or 4

# Choose Your Own 'xAL' Adventure

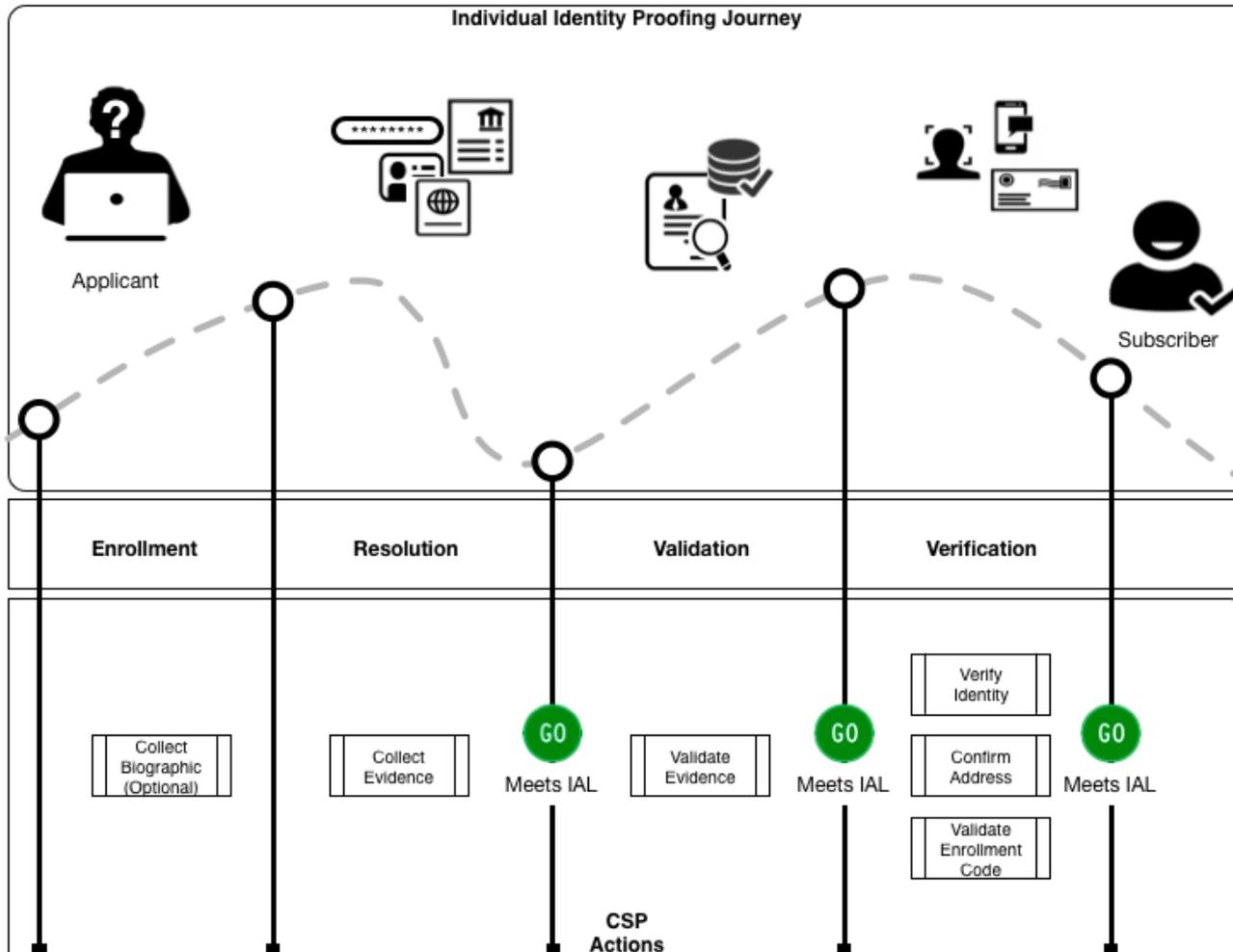




**SP 800-63A**

**Identity Proofing &  
Enrollment**

# A Stronger Identity Proofing Process



# Components of Stronger ID Proofing

- Clarifies methods for resolving an ID to a single person
- Evaluating and determining the strength of presented evidence
  - Unacceptable, Weak, Adequate, Strong, Superior
- Moves away from a static list of acceptable documents and increases options for combining evidence to achieve the desired assurance level
- Visual inspection no longer satisfactory at higher IAL
- TFS-related requirements are gone
- Reduced document requirements in some instances
- Clearer rules on address confirmation

# An Example

## IAL 2

### Evidence

- One (1) piece of SUPERIOR or STRONG evidence if the issuing source of the evidence, during its identity proofing event, confirmed the claimed identity by collecting two (2) or more forms of SUPERIOR or STRONG evidence; OR
- Two (2) pieces of STRONG evidence; OR

### Validate

- One piece of STRONG evidence plus two (2) pieces of ADEQUATE evidence
- Each piece of evidence must be validated with a process that is able to achieve the same strength as the evidence presented; For example, if two forms of STRONG identity evidence are presented, each evidence will be validated at a strength of STRONG.

### Verify

- Validation against a third party data service SHALL only be used for one piece of presented identity evidence.
- At a minimum, the applicant must be verified by a process that is able to achieve a strength of STRONG.

# Expanding & Clarifying Identity Proofing Options

- ✓ Virtual in-person proofing counts as in-person
- ✓ Remote notary proofing
- ✓ Selfie match
- ✓ Trusted referees (e.g., notaries)
- ✓ Traditional with KBV

# Knowledge Based Verification's Role in Identity Proofing

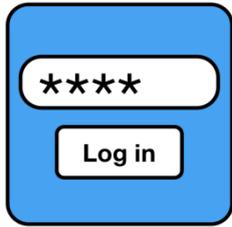
- No restrictions in the resolution phase of ID Proofing
- Highly restrictive in verification phase
  - Strict and clear rules on the use of KBVs
  - Definition of proper/allowable data sources
  - Prefers knowledge of recent Tx over static data
  - Cannot be standalone



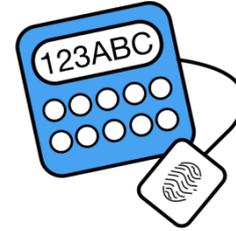
**SP 800-63B**

Authentication &  
Lifecycle Management

# Authenticators



Memorized Secrets



Multi-Factor OTP Devices



Look-up Secrets



Single Factor Cryptographic Devices



Out-of-Band Devices



Multi-Factor Cryptographic Software



Single Factor OTP Device



Multi-Factor Cryptographic Devices

# Password Guidance Changes

- Same requirements regardless of AAL
- SHALL be minimum of 8 characters.
- SHOULD (with heavy leaning to SHALL) be:
  - Any allowable unicode character
  - 64 characters or more
  - No composition rules
  - Won't expire
  - Dictionary rules
- SHALL - Storage guidance to deter offline attack (salt, hash, HMAC)

# Authenticator Guidance Changes

“Token” is out  
“Authenticator” is in



Server side biometric matching is in



OTP via SMS is deprecated



OTP via email is out



Pre-registered knowledge tokens are out



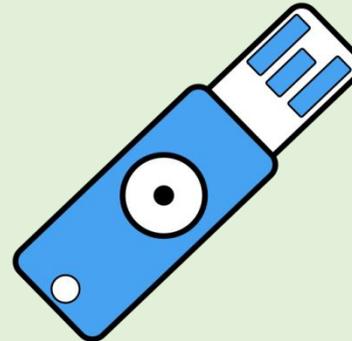
# New Authenticator at AAL3

Single Factor Cryptographic Device  
+ Memorized Secret Token

Example



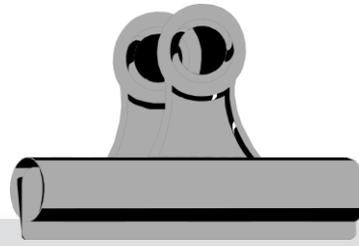
+





**SP 800-63C**

**Federation & Assertions**



## 800-63-C

# Federation & Assertions

Discusses multiple models & privacy impacts &

- 1 Requirements  
Many SHOULDs – document needs to be
- 2 Diagnostic
- 3 Modernized to include OpenID Connect
- 4 Clarifies Holder of Key (HOK) for the new AAL 3
- 5 Attribute requirements

# Attribute Claims vs. Values

## Maturity Model



## Old

Give me date of birth.  
Give me full address.

## New

I just need to know if they are older than 18.  
I just need to know if they are in congressional district X.

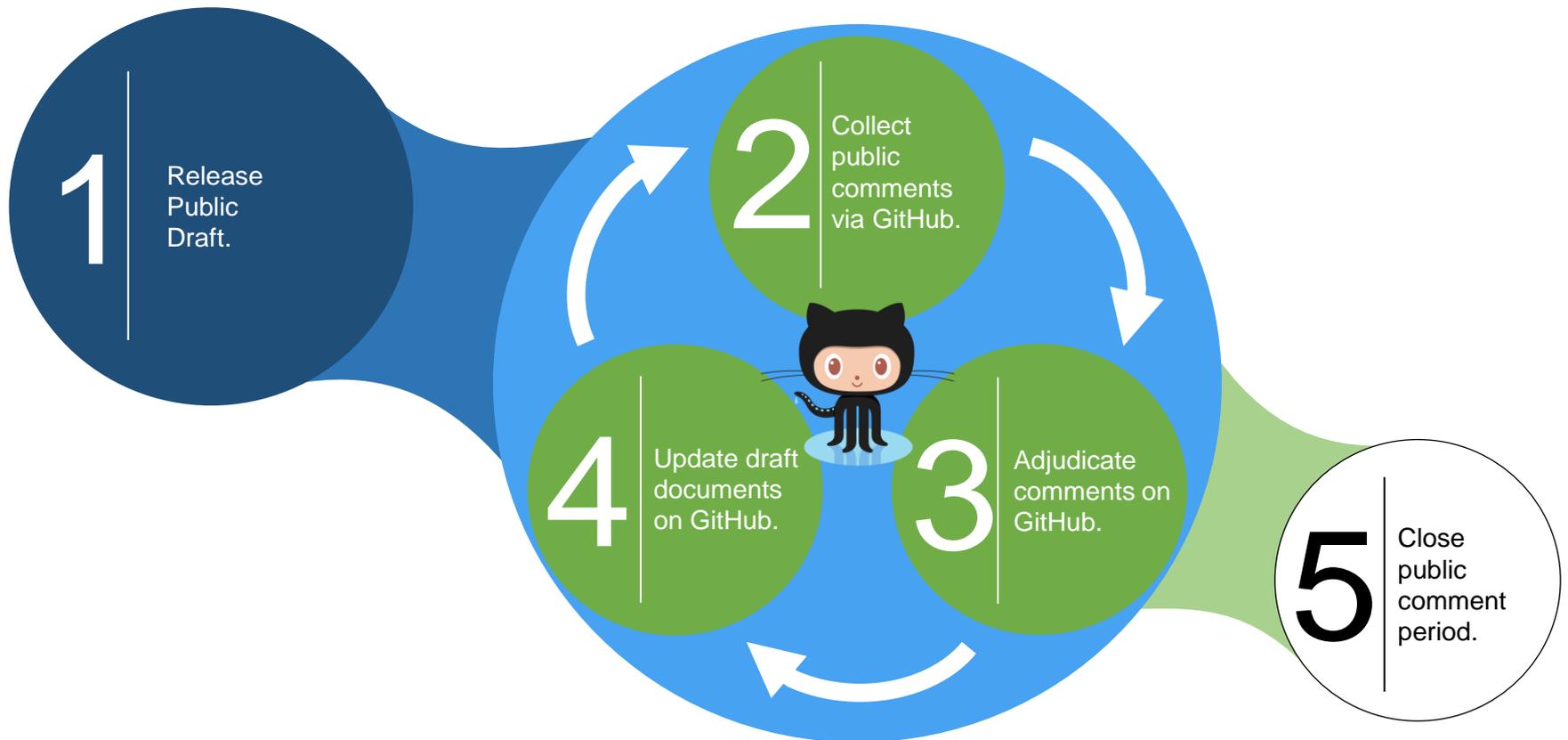
## New Requirements

**CSP** SHALL support claims and value API

**RP** SHOULD request claims

# Retaining the New Development Approach

*Iterative – publish, comment, and update in a series of drafting sprints*



# What's Next

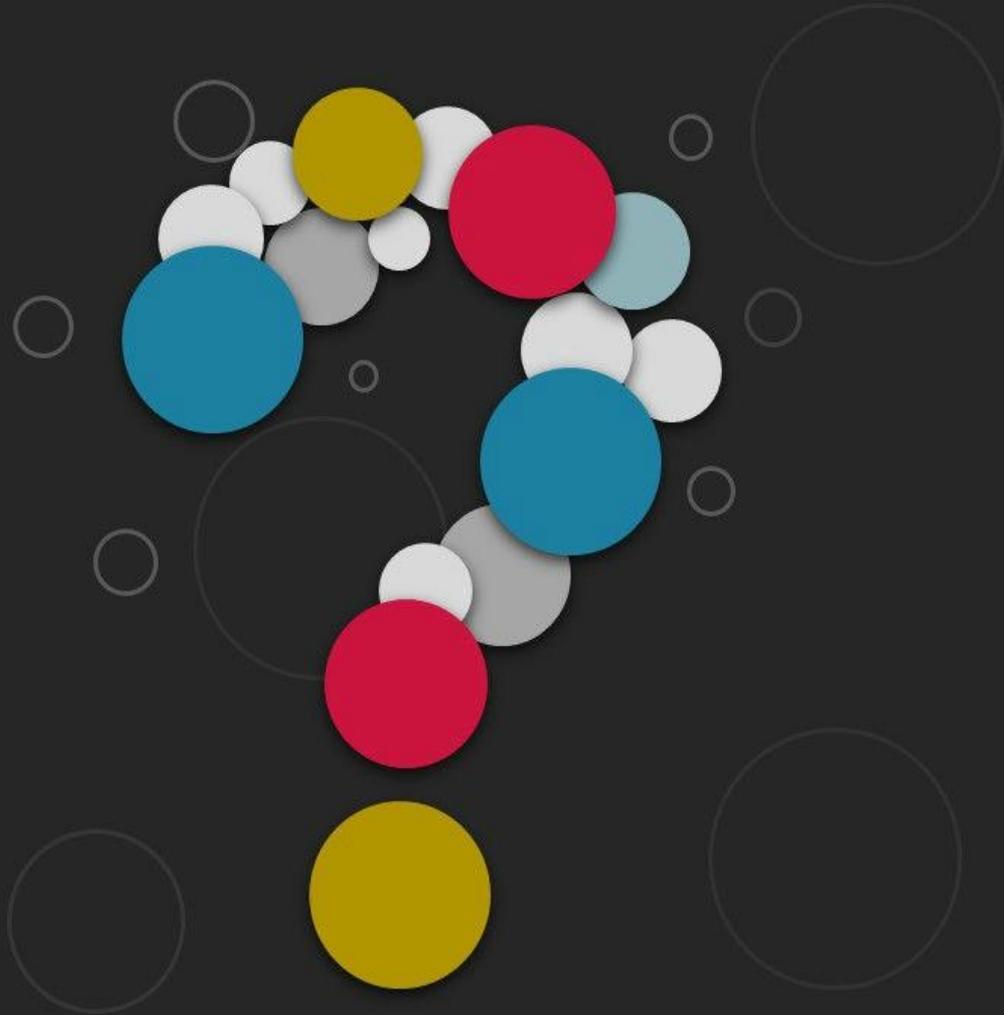
## Public Draft Comment Period

opens ~**October 13, 2016**  
closes **+60 days**

## Final Document

expected **Q2FY17**

# Questions





Virginia Information Technologies Agency

# Upcoming Events





## IS Orientation

**When: Thursday, September 29, 2016**

**Time: 9:30 – 11:30 am**

**Where: CESC , Room 1221**

**Presenter: Bill Freda**

**Register here:**

**<http://vita2.virginia.gov/registration/Session.cfm?MeetingID=10>**



*Virginia Information Technologies Agency*

# National Cybersecurity Awareness Month October 2016





# National Cyber Security Awareness Month



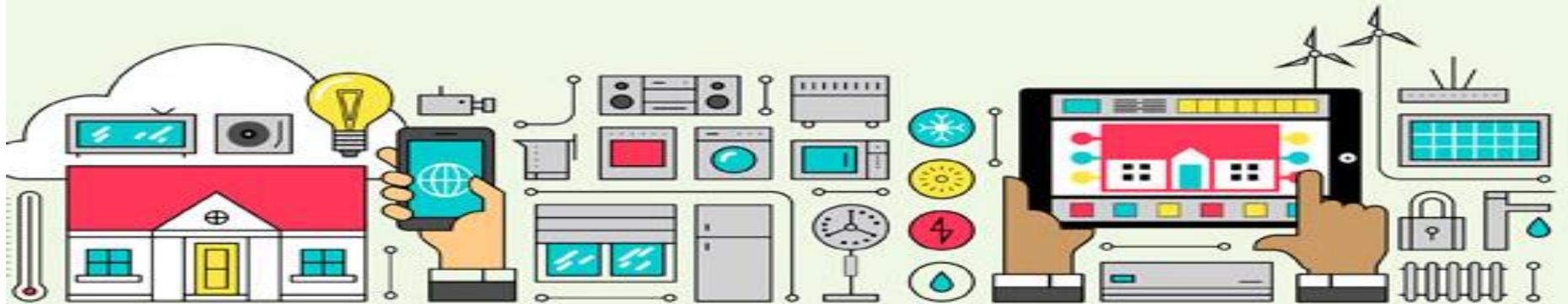
National Cyber Security Awareness Month



CyberAware

*securing our online lives is a*  
**SHARED RESPONSIBILITY**

*Get involved this October and empower our global digital society to use the Internet safely and securely.*





## Start Planning Now

### Weekly Themes

- |                       |   |
|-----------------------|---|
| Week 1: October 3-7   | Every Day Steps Towards Online Safety with Stop.Think.Connect.™ |
| Week 2: October 10-14 | Cyber from the Break Room to the Board Room                     |
| Week 3: October 17-21 | Recognizing and Combating Cybercrime                            |
| Week 4: October 24-28 | Our Continuously Connected Lives: What's Your `App'-titude?     |
| Week 5: October 31    | Building Resilience in Critical Infrastructure                  |



## Additional Resources

[www.stopthinkconnect.org](http://www.stopthinkconnect.org)

[ftc.gov/bulkorder](http://ftc.gov/bulkorder)

Order free resource materials from the Federal Trade Commission

[ww.staysafeonline.org/stay-safe-online/](http://ww.staysafeonline.org/stay-safe-online/)

[www.microsoft.com/security/default.aspx](http://www.microsoft.com/security/default.aspx)

[www.us-cert.gov/ncas/tips](http://www.us-cert.gov/ncas/tips)

[www.dhs.gov/national-cyber-security-awareness-month.](http://www.dhs.gov/national-cyber-security-awareness-month)



## Contact

**CommonwealthSecurity@vita.virginia.gov**  
**or**  
**Tina.Harris-Cunningham@vita.virginia.gov**



## Future ISOAG

**October 5, 2016 1:00 - 4:00 pm @ CESC**

**Speakers:**

**ISOAG meets the 1<sup>st</sup> Wednesday of each month in 2016**

# ADJOURN

## THANK YOU FOR ATTENDING

