Today’s Meeting...

Purpose: A briefing to describe Reduced SmartID Sign-On (RSSO).

Agenda:

Introductions

Review the Specifics:
  - Purpose of RSSO?
  - The Specifics:
    - What is Included in RSSO?
    - Background of RSSO?
    - What Will Change?
    - What Will Not Change?
    - When Will it Change?

Next Steps?

Questions…
Purpose of RSSO

- Employees will no longer have to remember all those login IDs and passwords
- RSSO enables employees to login to systems and applications using their SmartID and incorporates a COTS product which reduces the password burden for most applications
- Will improve the security posture of the IRS
- Will bring the IRS into compliance with Treasury & OMB mandates
- RSSO is an element of what was agreed to in the Workforce of Tomorrow initiative
• Three capabilities were combined into a single initiative called Reduced SmartID Sign-On (RSSO)
  • SmartID logon (logging into the network (LAN) with the HSPD-12 Smart card now called SmartID)
  • Reduction in password burden (managing logins/passwords for systems and applications)
  • Two Factor Authentication for Administrators (meets Treasury security controls – EC-14)

• Name Clarification:
  • ESSO – Industry term for Enterprise Single Sign-On products
  • SSO – Industry term for Single Sign-On products
  • RSSO – This IRS initiative > Combining “Reduced” Sign-On capability using the HSPD-12 SmartID
History of RSSO

- MITS and AWSS’s Credentialing & Identity Management Office began a 5000 person NBU pilot to use SmartID cards to enhance security and as a way to significantly reduce the password burden on IRS employees.

- The pilot represents all IRS business units to ensure a cross-section of users and is limited to NBU and BU Support personnel with SmartIDs.

- RSSO meets the HSPD-12 mandate for logical access controls and Treasury Enhanced controls EC-14 and EC-15 by enabling end-users to log into the computer by inserting their HSPD-12 SmartID.
What Will Change:

- Employees will simply insert their SmartID card into their computer and enter their Personal Identification Number (PIN) to gain access to their computers and applications. This replaces the traditional Ctrl-Alt-Del sequence with SEID and password.

- No longer have to enter logins/passwords for many applications and systems, eliminating the burden of keeping track of multiple, frequently changing passwords.

- Must remember to remove their SmartID from the card reader when they leave their workstation for breaks, lunch or leaving the office.

- Know their PIN: 6-8 numeric digits required for SmartID Sign-On – PIN will only change every 3 years.

- Employees may need to travel to a credentialing station if they need a PIN reset – PIN resets are not self-service (see HSPD12 MOU).
What Will Not Change:

- How Work is Performed on a Daily Basis

- Security Requirements:
  - The requirement to lock the workstation when away stays the same
  - Wearing/displaying the SmartID when not inserted in computer
  - The requirement to change passwords based on application or Security requirements

- Process will not change at this time for logging onto ERAP and EDE
When Will it Change:

Reduced SmartID Sign-On

- 5000 user pilot underway through 12/2009
- Production deployment to remaining employees in early CY2010 pending budget approval
- A phased approach to production deployment and continued close coordination with the Business POCs
Two Factor Authentication (TFA)

Two Factor Authentication (TFA) for System Administrators

500 Administrator pilot through 12/2010

Planning and testing continue for Two factor Authentication and RSSO implementation for Administrators (users with elevated privileges) – planned for completion by 2011
Next Steps:

- Development of communication strategy to provide program status to all stakeholders and customers
- Continue to develop Employee job-aids and FAQs
- Finalize negotiations so that we can expedite deployment to the bargaining unit employees
Your Concerns and Questions...