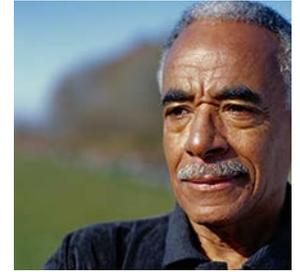




**2015 VA Privacy Matters
Symposium**

*Session 2:
Privacy Awareness*



June 9, 2015



Office of Information Security
Privacy and Records Management

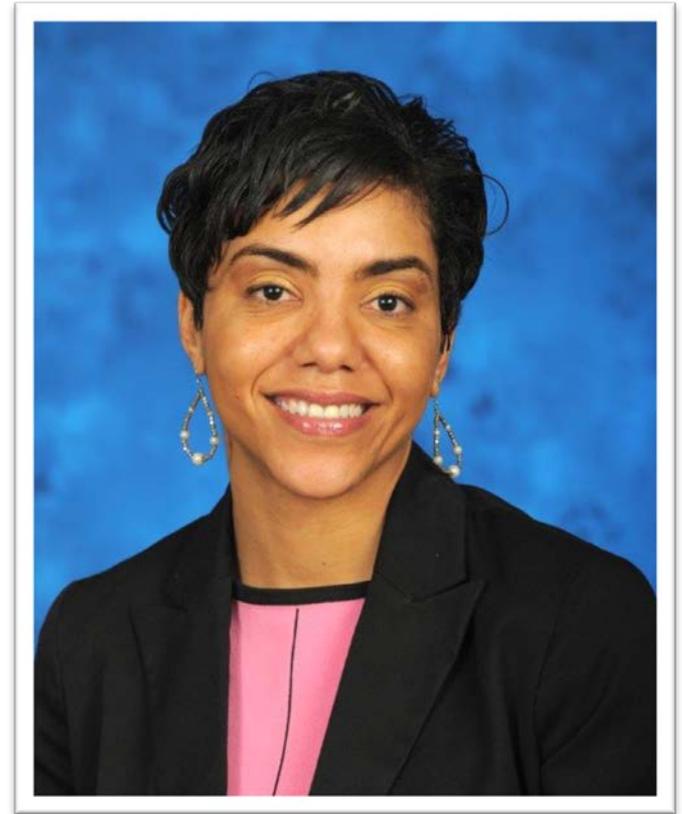
Administrative Items

- Do not use your computer microphone to participate in this meeting. Lync will be used only as a display. Please dial in using the following information:
 - Phone number: 1-800-767-1750
 - Conference ID: 24081
- Please mute your computer microphone and speakers. This will eliminate feedback on the line and make it easier for you and your colleagues to hear the presentation.
- The presenters will address questions at the end of the presentation. For those online, please feel free to type your questions into the Lync Instant Messenger.
- Send technical issues to VACOPrivacySpeakers@va.gov.

Moderator

Dominique Banks

Privacy Analyst and
Policy Lead for VA Privacy Service





Guest Panelists

Dianna Carr

Deputy Director

**National Protection and Programs Directorate
U.S. Department of Homeland Security**

Chalmer Rennie

Privacy Officer

**Veterans Benefits Administration
U.S. Department of Veterans Affairs**

Jeremy Maxwell, PhD

IT Security Specialist

**Office of the National Coordinator for Health IT
U.S. Department of Health & Human Services**

Kristen Lefevre

Senior Privacy Specialist

**Office of the Chief Privacy Office
U.S. Department of Education**



Dianna Carr

Deputy Director

National Protection and Programs Directorate

U.S. Department of Homeland Security

Privacy Awareness Symposium

Building Privacy Awareness

PRIVACY

Dianna Carr

Deputy Director, Privacy

Department of Homeland Security

National Protection and Programs Directorate



What We Do...

- DHS HQ Privacy Office
 - First statutorily required privacy office in any federal agency
 - Sets DHS-wide policies
- NPPD Office of Privacy
 - Plans and develops privacy compliance documentation
 - Develops privacy policies specific to NPPD mission
 - **Provides guidance, training, and awareness**
 - Ensures compliance with DHS Incident Handling policies and procedures



Privacy Guidance

- DHS HQ Privacy Office
 - DHS Handbook for Safeguarding Sensitive PII
 - Privacy Incident Handling Guidance
- NPPD Office of Privacy
 - Privacy Incident Handling SOP
 - Safeguarding Sensitive PII Factsheet
 - Safeguarding PII While Teleworking Factsheet
 - Email Best Practices
 - Understanding Cookies Factsheet
 - Privacy Incident Reporting Cards
 - Privacy Tips for Contracting Officer Representatives
 - How to Incorporate the FIPPs into Correspondence and Task Management
 - Checklist for Safeguarding PII during Office Moves
 - SharePoint and Privacy Guidance



Telework Best Practices

When	Do's	Don'ts	Why
Before you telework...	<p>✔ Plan ahead to ensure that sensitive documents can be safely accessed remotely. Organize your files so that they are easily accessible from the DHS secure portal, http://connect.dhs.gov. Use DHS-approved, portable electronic devices, which are encrypted, adding a layer of protection to your data.</p>	<p>✘ Don't forward emails to your personal email account or use non-approved portable electronic devices. Have a back-up plan in case you experience issues with network connectivity, but never transfer or download data to your personal computer, personal email account, or to non-encrypted devices.</p>	When you remove data from the DHS network, DHS cannot protect it. There may be instances where you need to send sensitive PII to job applicants or individuals without DHS accounts, but it must be encrypted or password protected. To send it unencrypted is considered a privacy incident (or data breach).
	<p>✔ Obtain authorization from your supervisor to take home sensitive documents, and make sure documents containing sensitive PII are marked "For Official Use Only" or "Privacy Data." Inventory your hard copy documents when you leave the office and before you return them to the office.</p>	<p>✘ Don't take sensitive PII home that you do not need. Limit your removal of sensitive PII from the office to only that information that is relevant and necessary to the work outlined in your telework agreement.</p>	Hard copy documents are easily lost or misplaced, putting sensitive PII at risk. Conducting an inventory and properly marking documents helps mitigate the risk of unauthorized disclosure.
Transporting documents...	<p>✔ Be able to secure sensitive data when not in use. If you must leave your laptop or hard copy documents inside a vehicle, leave them inside a locked trunk and only for short periods of time. When traveling, place sensitive data in a hotel safe when not in use.</p>	<p>✘ Don't leave your laptop or hard copy documents unattended overnight. Maintain accountability of your data by ensuring documents are secured when not in use.</p>	Failure to maintain accountability of sensitive PII can lead to loss, theft, or misuse, resulting in a privacy incident.
At home...	<p>✔ Log in through the DHS secure portal, http://connect.dhs.gov. Organize your work space at home such that work files are separate from personal files and can be properly safeguarded.</p>	<p>✘ Don't transfer files to your home computer or print agency records to your home printer. </p>	Your home computers, printers, faxes, and copiers all contain internal storage or "hard drives." Even when these devices are disposed of, the information stored within is vulnerable.
	<p>✔ Take advantage of DHS collaboration tools such as SharePoint. Ensure shared files contain appropriate security controls to limit access to sensitive data.</p>	<p>✘ Don't store sensitive PII in SharePoint unless your site has been approved for such use. Access must be limited to those that have an official need to know.</p>	Collaboration tools provide quick, easy access to data, but without proper security controls, can lead to data winding up in the wrong hands. Sharing sensitive PII with unauthorized users is considered a privacy incident.
	<p>✔ Secure your data, and ensure other household members do not have access to it. Organize your work space at home such that Government property and information are kept separate from personal property and can be properly safeguarded.</p>	<p>✘ Don't leave files containing sensitive data lying out in the open. Never leave sensitive PII in view of children, spouses, or visitors. Sensitive PII should be secured in locked cabinets and your computer/Blackberry should remain locked when not in use.</p>	Failure to properly secure sensitive records could result in inadvertent sharing of sensitive PII.

Telework Resources:

- DHS IT Help Desk: 1-800-250-7911
- DHS Remote Email Access: <http://connect.dhs.gov>
- webTA: <https://wta.hs.nrc.usda.gov/webta>
- NPPD SharePoint Sites: <http://nppd-sp.dhs.gov>
- NPPD Telework website: <http://dhsconnect.dhs.gov/org/comp/nppd/ora/Pages/NPPDTelework.aspx>

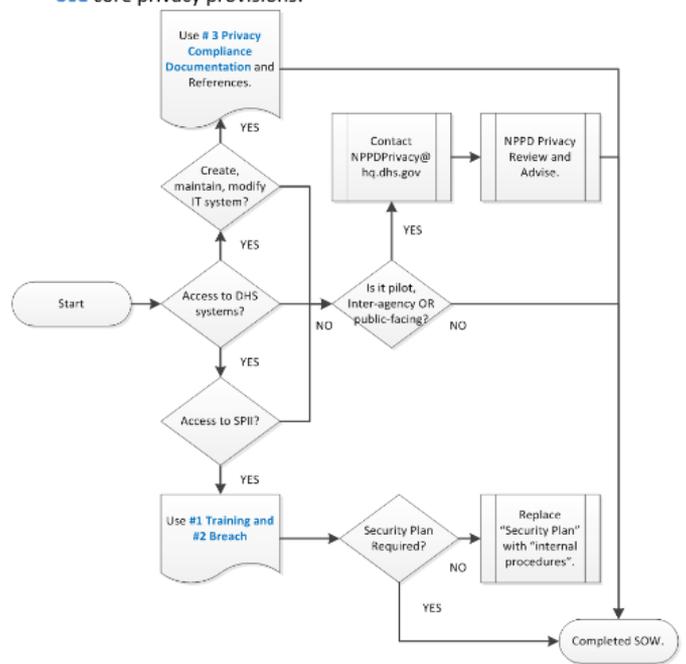


Privacy Tips for CORs

Establish Privacy Requirements

- ✓ **Identify** privacy-sensitive contracted activities:
 - Access to IT resources
 - New systems, programs
 - Pilots
 - Research/testing

- ✓ **Use** core privacy provisions:



- ✓ **Cite** FAR/HSAR Clauses:
 - FAR 52.224-1/2 Privacy Act Notification / Privacy Act
 - FAR 52.239-1 Privacy or Security Safeguards
 - HSAR 3052.204-70 Security Requirements for Unclassified IT
 - HSAR 3052.204-71 Contractor Employee Access to IT Systems

Privacy Tips for CORs

Protect Sensitive PII

- ✓ **Minimize** the use of SPII:
 - Request only the number of positions and the position rate, if generating prices from a seniority list
 - Remove the address until delivery must be performed, for purchase orders delivered to home offices
 - Secure all PII handled regarding the request, maintenance, or withdrawal of personnel suitability or security clearance
- ✓ **Secure** SPII by...
 - Encrypting or password protecting emails and attachments, and send the password "out of band"
 - Checking the auto-fill of recipients' email addresses
 - Locking up hard copies of PII
 - Disposing in a designated bin or shredding
 - Not leaving documents on printers or faxes
 - Not emailing PII to your personal email address
- ✓ **Unsure?** When in doubt, protect PII, when it ...
 - Shouldn't be seen by an unintended recipient
 - Could cause embarrassment
 - Could lead to identity theft
 - Could lead to social engineering or phishing attempts
- ✓ **Report** suspected and/or confirmed privacy incidents to your Supervisor and the DHS Help Desk at 1-800-250-7911.

Have questions? Contact the NPPD Office of Privacy at NPPDPrivacy@hq.dhs.gov.



Privacy Training

- DHS HQ Privacy Office
 - Privacy at DHS: Protecting Personal Information
- NPPD Office of Privacy
 - Privacy 101 (receive collateral credit for annual mandatory training)
 - New Employee Orientation
 - Cybersecurity Information Handling
 - Privacy and Acquisitions
 - Social Media Requirements & Operational Use of Social Media Training
 - Other role-based training (e.g., field personnel, HR, etc.)



Privacy Awareness

- DHS HQ Privacy Office
 - Annual Privacy Workshop
- NPPD Office of Privacy
 - Privacy Week
 - Privacy and Technology Workshop
 - Quarterly Privacy Training Events
 - Privacy Update
 - Privacy Tips and Articles



NPPD Privacy Week Awareness Event

NPPD Privacy Week will be held from October 22-26, 2012

This year's theme: *Privacy by Design. We bake privacy protections into everything we do!*

Got
COOKIES?

Cookie [kook-ee] noun¹

- 1. A small cake made from stiff, sweet dough rolled and sliced or dropped by spoonfuls on a large, flat pan and baked.
- 2. A message, or segment of data, containing information about a user, sent by a Web server to a browser and sent back to the server each time the browser requests a Web page.

Join us on October 4, 2012 from 11:00am – 1:00pm at 1616 N. Fort Myer Dr.
Room 668 to learn about this year's exciting events.

This is a great opportunity to learn about cookies...while eating cookies!

¹<http://dictionary.reference.com/browse/cookie>



NPPD Office of Privacy

Privacy by Design.

We bake privacy protections into everything we do.

National Protection & Programs Directorate

PRIVACY WEEK

OCTOBER 22-26, 2012

Save the date(s) for these special events and look for announcements and additional information throughout the week!

MONDAY, OCTOBER 22

Kick-off & Welcome Remarks
 Rand Beers
 Under Secretary, NPPD

Keynote Speaker
 Jonathan Cantor
 Acting Chief Privacy Officer,
 DHS
 12:00 pm - 1:00 pm
 1616 N. Fort Myer Drive
 Room 1890
 Arlington VA, 22209

TUESDAY, OCTOBER 23

Be a Smart Cookie:
Prevent Identity Theft at Any Age
 10:00 am - 11:00 am
 1110 N. Glebe Road
 Room 1128
 Arlington VA, 22201

Kneading Privacy into Operations
 2:00 pm - 3:00 pm
 1421 Jefferson Davis Highway
 Room 01-002
 Arlington VA, 22202

WEDNESDAY, OCTOBER 24

"How-to" Bake Privacy Protections into Technology
 12:00 pm - 2:00 pm
 1616 N. Fort Myer Drive
 Room 1890
 Arlington VA, 22209

THURSDAY, OCTOBER 25

Recipes for Respecting Privacy while Monitoring Social Media
 10:00 am - 11:00 am
 800 N. Capitol Street NW
 Maritime Conference Room
 Washington DC, 20002

If you have any questions related to Privacy Week, please email NPPDPrivacy@hq.dhs.gov.

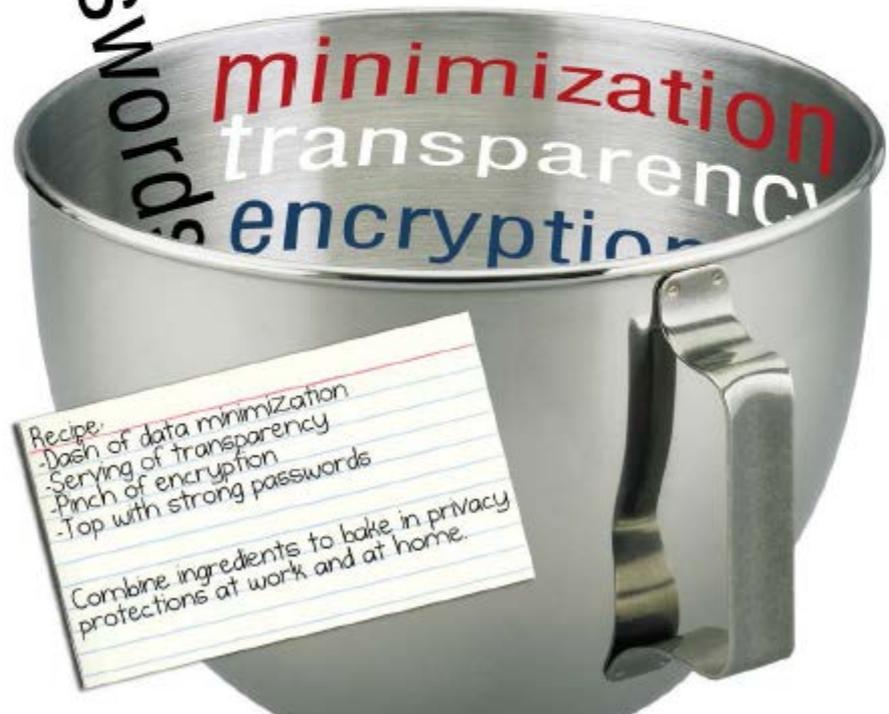
NPPD Privacy Week

October 22-26, 2012

Privacy by Design.

We bake privacy protections into everything we do.

passwords



Recipe:
 -Dash of data minimization
 -Serving of transparency
 -Pinch of encryption
 -Top with strong passwords
 Combine ingredients to bake in privacy protections at work and at home.



NPPD Office of Privacy

NPPD Privacy Week

October 22-26, 2012

Privacy by Design.

We bake privacy protections
into everything we do.



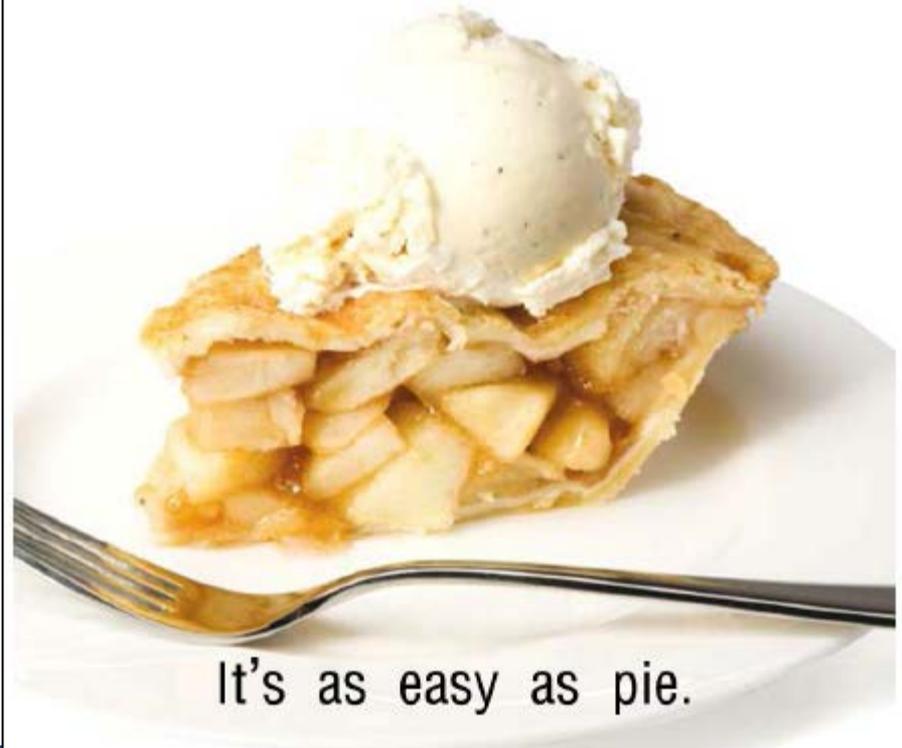
Make privacy a
core ingredient,
not a topping.

NPPD Privacy Week

October 22-26, 2012

Privacy by Design.

We bake privacy protections
into everything we do.



It's as easy as pie.



National Protection & Programs Directorate

Privacy and Technology

Workshop!

Featuring demonstrations on:

Social Media

PCII

Biometrics

Cybersecurity



Online Holiday Shopping Tips

December 5, 2013

2:00pm to 3:30pm • Room 1890

1616 N Fort Myer Dr, Arlington VA 22209

For more information, contact NPPDPrivacy@hq.dhs.gov

*Keep your personal information under wraps –
for the holidays and every day...*



Federal CIO Council - Privacy Training and Awareness Best Practices

Search The MAX Community

All ▾



OPEN - EXECUTIVE BRANCH ▾

E-Govern > Home > E-Gov Co > Federal CIO Council Privacy Committee > Federal CIO Council - Privacy Training and Awareness Best Practices (5) ▾

✎ (2) 💬 (0)

Edited By Steven Richards(DHS) on May 03, 2012 at 04:22 PM ▾

Edit

Add Content ▾

Favorites ▾

Share

Watchers (4) ▾



Home

Privacy Training

Privacy Awareness

Metrics

Privacy Resources

Introduction

This site is a resource for all federal privacy offices developing or expanding a privacy training and awareness program in order to build a culture of privacy within an organization. Studies on the causes of data breaches show that most occur due to unintentional error by an organization's staff, rather than malicious acts. Therefore, staff can and should be trained to protect personal information or Personally Identifiable Information (PII).

- [DHS:Top 5 Mistakes of Privacy Awareness Programs \(PDF\)](#)
- [DHS:Data Beach Mistakes Feared More Than Hackers by Compliance Professionals \(PDF\)](#)

To create an effective privacy training and awareness program with limited resources, follow the best practices detailed on this site.

Feedback

If you have questions or want to submit content to be considered for publication on this site, please email Steve Richards at: steven.richards@hq.dhs.gov

Background

A privacy training and awareness program is more effective if your privacy office is founded on a privacy risk management framework [DHS:e.g., the Fair Information Practice Principles], as well as good privacy policies.

Effective privacy stewardship includes:

1. Organizational commitment to privacy
2. Privacy risk mitigation in operations

Questions?
Feel free to contact:
dianna.carr@hq.dhs.gov





Chalmer Rennie

Privacy Officer

Veterans Benefits Administration

U.S. Department of Veterans Affairs

Veteran Benefits Administration Privacy (VBA) Awareness

Chalmer Rennie
VBA Privacy Officer

VBA Privacy Awareness

User Error and Need for Security Awareness

- Veteran Benefits Administration (VBA) knew the weakest element in our security were people.
- That's probably the weakest part of any organization. You can have all the security protocols , massive email filtering, but stuff is still going to get through and criminals are still going jump on that.
- User education can go a long way to keeping outsiders off the network, but it isn't a silver bullet.
- In the past, prior to implementing the awareness program, VBA had to deal with various user error vulnerabilities . Those were mostly improper disclosure of Social Security Numbers and fraud due to disclosures. The need for an awareness program was made abundantly clear when a data set was improperly disclosed.

VBA Privacy Awareness

User Error and Need for Security Awareness

- VBA had to keep the materials basic, so that the information was easily understood and the technical aspects were obtainable to anyone, no matter their personal skill set.
- Security awareness programs are only one piece of a larger security puzzle. By the time an improper disclosure is made, security awareness has failed. Now the weakest-link in the chain now has an active role in defense.
- If the users are trained, or to use a stronger term, conditioned to prevent an improper disclosure, there is a greater chance veteran PII is protected..
- However, the main takeaway is that if the human element is educated and trained, or at least better prepared, then improper disclosures are dramatically minimized.

VBA Privacy Awareness

VBA Developed Security Awareness and Metrics

- Veteran's Benefits Administration (VBA) developed long term training schedule for Privacy Awareness, it was important to measure the awareness program by utilizing metrics. The reason metrics were vital to our security awareness program is because VBA employees as whole needed to understand how the program has improved with security awareness and to measure change.
- VBA measured the number of employees who complete/did not complete the security awareness training program.

VBA Privacy Awareness

VBA Developed Security Awareness and Metrics

- Test results of VBA employees for before and after training and VBA looks at which topics impacted security awareness, employee knowledge of policies, etc.
- Finally, VBA measures the number of employees who fall victim to phishing scams, viruses, improper disclosures etc.
- Having the metrics for the VBA security awareness program helps VBA focus in on the areas that needs improving.



Jeremy Maxwell, PhD

IT Security Specialist

Office of the National Coordinator for Health IT

U.S. Department of Health & Human Services



The Office of the National Coordinator for
Health Information Technology



Privacy Matters Symposium: A Conversation in Privacy

Jeremy Maxwell
IT Security Specialist



Office of the Chief Privacy Officer

The Office of the National Coordinator for
Health Information Technology

Does it work?
Is it enough?



What Do All These Say?

Security Alert



Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.



The security certificate not chosen to trust. View you want to trust the ce

Warning - Security

The application's digital signature has been verified. Do you want to run the application?



User Account Control



Do you want to allow the following program from an unknown publisher to make changes to this computer?

Program name:
Publisher:
File origin:

Show details

Security Information



This page contains both secure and nonsecure items.

Do you want to display the nonsecure items?

Yes

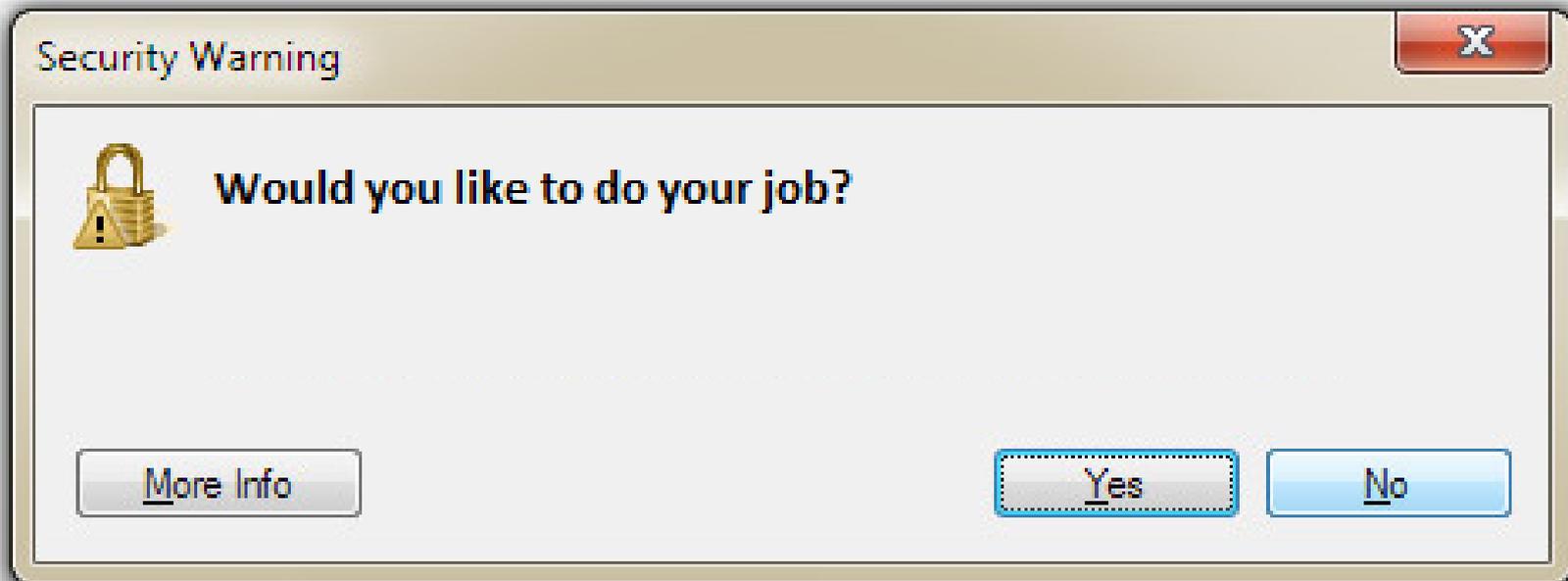
No

More Info

Run

Cancel

[More Information...](#)



- Make it easy to preserve privacy; hard to endanger privacy
- Traditional privacy skillset vs. security skillset
- More human element needed in security, more technology needed in privacy
- Usability is key

Making Privacy Real for Individual Contributors

- Contextual privacy
- *Post hoc vs. a priori*
- NIST draft privacy framework
 - Predictability, manageability, disassociability

- Make sure they understand your policy positions
- Table top exercises of privacy events





Kristen Lefevre

Senior Privacy Specialist

Office of the Chief Privacy Officer

U.S. Department of Education

Guest Panelists Q&A

Dianna Carr

Deputy Director

National Protection and Programs Directorate
U.S. Department of Homeland Security

Chalmer Rennie

Privacy Officer

Veterans Benefits Administration
U.S. Department of Veterans Affairs

Jeremy Maxwell, PhD

IT Security Specialist

Office of the National Coordinator for Health IT
U.S. Department of Health & Human Services

Kristen Lefevre

Senior Privacy Specialist

Office of the Chief Privacy Office
U.S. Department of Education

Questions



Thanks for Attending!

- Thank you for attending the 2015 VA Privacy Service “Privacy Matters” Symposium.
 - We value your feedback, opinions and comments!
 - After this session, you will receive a short questionnaire via email. Please take a moment to complete upon receipt.
- To self-certify Lync Meeting attendance in the Talent Management System (TMS), search:
 - **Item Title:** VA Privacy Symposium 2015: Session II - Building Privacy Awareness (Live Webinar)
 - **TMS ID:** VA 3941945
- Visit the new VA Privacy Service website at <http://www.oprm.va.gov> to learn more about Privacy within VA.