

DO Off-Boarding Session Agenda – Tuesday January 10, 2017

Welcome

Mary Lhotsky, Director of Communications, Treasury Management and Budget

Navigating the Off-Boarding Site & Tools (P4P Process) and Human Resources

Vernetta Wilkins and Stacie Gibbs, Human Resources Office

Insider Threat and Counterintelligence Awareness Briefing

Lara Murad, Office of Counterintelligence

PIV Card and Office Keys

LaDaryl Scott, Office of Physical Security

Records Management

Bertrand Tzeng, Director, Records and Information Management, Office of Privacy, Transparency, and Records

Closing Remarks

Open House/Booths for Questions:

Public Transportation Incentive
Program (PTIP)

Travel Card/Purchase Card

I.T. Equipment Returns

Benefits (Insurance, etc.)



DEPARTMENTAL OFFICES
MANAGEMENT



Navigating the Off Boarding Site & Tool Kit (P4P Process)

Office of Human Resources

Off-Boarding/Leaving Treasury

[Overview](#)

[Off-Boarding Checklist](#)

[F.A.Q.'s](#)

[Senior Executives](#)

An effective and consistent off-boarding process plays an important role in protecting the interests of the exiting employee and the Department. The resources on this page will help employees, key contacts, and supervisors identify the necessary tasks that must be completed prior to an employee's departure.



Off-Boarding Toolkit

[Points of Contact](#)

[Helpful Links](#)

[Forms](#)

STEP 1:
10+ DAYS
BEFORE
DEPARTURE

Give Notice of Departure

Enter the Exit Request in P4P and Separation Action in HR Connect.

STEP 2:
5-10 DAYS
BEFORE
DEPARTURE

Complete Briefings

Schedule and obtain all applicable briefings (e.g. Security, Ethics, Records).

STEP 3:
2-3 DAYS
BEFORE
DEPARTURE

Return All Treasury Property

Return portable IT devices, PIV badges, travel or purchase cards, library materials, room keys, etc. to the appropriate POCs (see Off-Boarding Checklist).

STEP 4:
LAST DAY
AT TREASURY

Submit Off-Boarding Checklist

Once the Off-Boarding Checklist has been completed, click "Submit."

Need help getting started? Enter Exit Request in [P4P](#)

For any general process questions, please contact (OHR), phone: (202) 927-4800

Human Resources

Office of Human Resources

HR Exit



R
e
m
i
n
d
e
r
s

Leaving Agency

31-days extended coverage

60-days to enroll in TCC

Last Check recvd normal pay cycle

Annual Leave lump sum recvd est
2weeks after final paycheck has
been issued

House Cleaning Items

Transfer/Reassigning

Print last leave and earning
statement

Print close out performance rating

Update personal contact info in
HRC

Complete Exit Survey



Human Resources
Office of Human Resources

For more information regarding your benefits please contact your servicing Specialist at the Bureau of Fiscal Services

If your last name begins with:

A-C, call Ashley Wagner at 304-480-8996 or via email Ashley.Wagner@fiscal.treasury.gov

D-H, call Janice Burrows at 304-480-8207 or via email Janice.Burrows@fiscal.treasury.gov

I-M, call Jennifer Baldwin at 304-480-8149 or via email Jennifer.Baldwin@fiscal.treasury.gov

N-R, call Michele May at 304-480-8315 or via email Michele.May@fiscal.treasury.gov

S-Z, call Craig Huffman at 304-480-8192 or via email William.Huffman@fiscal.treasury.gov



Insider Threat and Counterintelligence Awareness

DO Off-Boarding Session



DEPARTMENTAL OFFICES
MANAGEMENT



Post-Treasury Counterintelligence Considerations

Handling Sensitive or Classified Information

- Sensitive or classified information should NOT be removed from Treasury without prior approval
 - Contact recordsmanagement@treasury.gov for questions regarding unclassified info
 - Contact sso@treasury.gov for questions regarding classified info

- Remember to de-conflict any work-related documents you wish to retain to avoid any problems

- Avoid forwarding Treasury emails to your personal accounts

- It is highly recommended that you submit your resume for review to avoid unauthorized disclosures (this is required for OIA employees)
 - Contact prepub@treasury.gov for a prepublication review



Insider Threat Case Study: Charles H. Eccleston

Charles H. Eccleston

- Former Department of Energy and Nuclear Regulatory Commission (NRC) employee arrested in Jan 2011
- Pled guilty in Feb 2016
- Faces up to 30 months in prison and a \$95,000 fine

What Happened?

- Eccleston attempted to hack federal agency computers to steal and then sell nuclear secrets to Iran, China, and Venezuela
- Fired from his job at the NRC in 2010, Eccleston had been living in the Philippines since 2011
- He came to the attention of the Federal Bureau of Investigation in 2013 when he entered a foreign embassy in Manila and offered to sell a list of over 5,000 email accounts of officials, engineers, and employees of a U.S. government energy agency
- In January 2015, Eccleston attempted to send dozens of spear-phishing emails to former colleagues containing malware with the intention of extracting classified nuclear information

So What?

- ✓ Who could become an insider threat? **Anyone with authorized access to U.S. Government resources who uses that access—either wittingly or unwittingly—to harm national security. Insider threats can have far reaching consequences and impacts on national security**
- ✓ Can you still be an insider threat post-employment? **Yes**



Post-Employment Counterintelligence Threats

- Offers of Foreign Employment
 - Former U.S. government employees are often targeted for collection by foreign intelligence entities with offers of travel accommodations, high salaries, and special designated positions
 - Aggressive interest in your past clearance level from a foreign employer is a red flag
- Social Media
 - Use discretion when posting information about your experience and access; it could increase your risk of being targeted
- Reporting to the Office of Counterintelligence
 - If you experience unusual encounters with foreign contacts that raise concerns, contact us (not mandatory, but encouraged)



Office of Counterintelligence

Hotline: 202-622-1348

Email: CI@treasury.gov



Office of Physical Security

DO Off-Boarding Session



DEPARTMENTAL OFFICES
MANAGEMENT



- What to do with your PIV Card
 - Leave your PIV card at any Main Treasury Complex (building or Annex) entry or exit location.
 - Drop your PIV card in the card slot or give it to the Secret Service officer.
- What to do with your office keys
 - Main Treasury office keys should be returned to the Main Treasury Pass & Lock Office, Room MT 1015, Monday – Friday, 8:00 a.m. to 2:00 p.m.

**Contact: TPA@Treasury.gov or
LaDaryl Scott
(202) 622-3063**



Records Management

Office of Privacy, Transparency,
and Records



DEPARTMENTAL OFFICES
MANAGEMENT



Before Traveling

01



Planning your departure

02



Preparing to go

03



Suggested steps

What may I take when I leave?

- Publicly-available materials
- Outlook contacts
- Personal documents

Non-public information: Treasury policy prohibits removal



What steps should I take?

- Complete the Treasury departure form (TD F 80-05.5)
- Contact the DO Help Desk for any Outlook items
- Separate personal documents and publicly available materials



What should I expect?

- Executives: PTR will contact you for an exit interview
- GS employees: You will receive the departure form and instructions via email

Contact PTR if you have any questions
(RecordsManagement@treasury.gov)



Ensure records will be properly maintained

- What is a record? Information that is –
 - Made or received to comply with a law or to conduct public business, and
 - Being preserved because it –
 - Is evidence of Treasury policy, decisions, and activities, or
 - Contains information of value
- What form can a record take?
 - Emails, electronic documents, and paper files

What is not a record?

- Non-records: Information that—
 - Was not made or received to conduct public business
 - Is neither evidence of Treasury policy, decisions, or activities, nor contains information of value
 - Or is merely a convenience copy
- Personal documents:
 - Belong to an individual
 - Were not used to conduct agency business

Suggested steps

Best clean-up practices

- Minimize your:
 - Non-records
 - Personal documents (and keep them separate from records)
 - Transitory documents (<180 day value)
 - Paper files
- Avoid storing records on local/shared drives
 - Keep records on your team's SharePoint site
 - Keep sensitive records to SharePoint MySite (e.g. personally identifiable information)



Suggested steps for email

Best clean-up practices for email

- Minimize your -
 - Non-records
 - Personal email (forward to your personal account)
 - Transitory email (<180 day value)
- Empty the Deleted Items folder regularly, but –
 - **Do *not* use it as a storage folder** (especially for records)
 - **Do *not* delete any email that is subject to a litigation hold**



Bon Voyage!

For more information, contact:

Office of Privacy, Transparency, and Records
Records and Information Management team
RecordsManagement@treasury.gov



Closing Remarks

Mary Lhotsky

Questions ?



Please take advantage of the Open House / Information Booths

