US BICES-X Training

The overall classification of this presentation is **UNCLASSIFIED**

Presented by: Gregory Morton
US BICES-X Trainer

V5.3.1

Break for a Security Reminder

- Remove all personal electronics from the room
  - Phones, Cameras, Fitbits, smart watches etc.
- Ensure all parties have the applicable security clearance requirements *(US Standards)*
- Secure the room
- Conduct introductions of all users

Overview

- Consolidated Dissemination Center-Pacific (CDC)
- Overview of Tools
- Demonstration of Tools
- Network Accounts
- Service Center West (SCW)

US BICES-X Mission and Purpose

- The DoD requires an enduring, secure information sharing capability with global partners
- US BICES-eXtended S//REL services to the coalition mission partners of the Combatant Commands
- US BICES-eXtended is capable of secure bilateral releasable communications

US BICES - Extended Enterprise

- USAF Program of Record which originated from an Office of the Undersecretary of Defense for Intelligence (OUSD-I)
- Assembly of SECRET REL, intelligence-sharing global networks
- Standardized communications system that allows for timely availability of intelligence to U.S. and participating partner nation organizations

US BICES-X is the communication backbone for coalition-building in a crisis

- **Basic sharing agreements established**
- **Network in place**
- **Instantaneous virtual Coalition capability**

Consolidated Dissemination Center-Pacific (CDC)

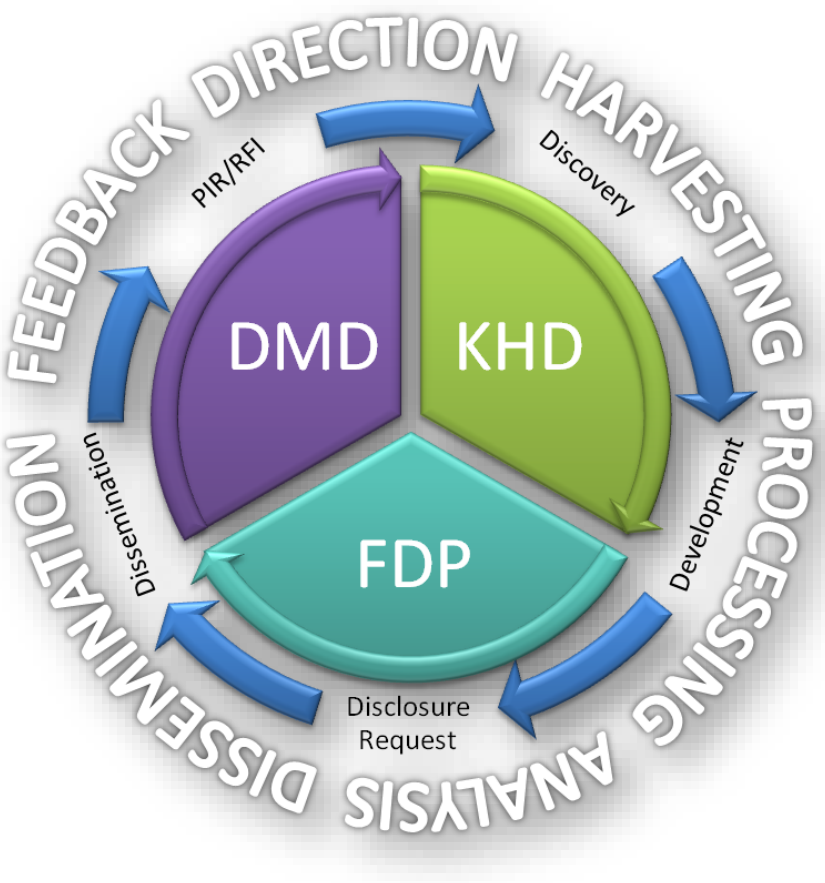
US BICES-X CDC Concept / Mission

The CDC mission is to facilitate the dissemination of *releasable* US intelligence information to foreign partners on US BICES-X Enterprise Networks

- CDC functions within the US BICES-X Enterprise:
  - Seek out releasable US products dissemination on the Enterprise Networks
  - Metatag disseminated products using NATO Intelligence Projects Interoperability Working Group (IPIWG) standards
  - Build enduring relationships with US agencies to facilitate greater information sharing

CDC-Pacific Background / Mission

Assist in developing releasable information for USINDOPACOM & Partners



CDC-P is divided into three teams:

- Knowledge Harvesting & Development (KHD)
  - – Searches, based on customer generated RFI's, for information that supports engagements
- Foreign Disclosure Processing (FDP)
  - – Facilitates USINDOPACOM FDO by submitting and tracking release requests with Original Classification Authorities
- Data Management & Dissemination (DMD)
  - – Disseminates FDO approved information to US BICES-X
  - – Metatags products using IPIWG standards

Consolidated Dissemination Center - Pacific

Building 398, Makalapa, Pearl Harbor

Commercial: **+1 808-473-6062**

US BICES-X: **3880**

NIPR: CDCP_analyst@dodiis.mil

US BICES-X: CDCP_analyst@***.cmil.mil

Operating Hours:

Local Time: 2300-1100 Monday (PM) – Saturday (AM)

HST: 0500-1700 Monday – Friday

***

After USINDOPACOM hours contact:

Coalition Support Service Desk

COMM: +44 1480 84 2815

NIPR: osd.molesworth.osd.mbx.usbices-coalition-service-desk@mail.mil

Overview of Tools

Overview of US BICES-X and Tools

- Established networks enable secure communication and collaboration between USINDOPACOM and participating nations
  - The suite includes computers, VoIP phones, VTC, printers, and scanners at the SECRET//REL level
- SYSTRAN translation tool
- Four methods for sharing information
  - **Shared Folders**: share, store & collaborate on products
  - **Product Library**: CDC-P has approved products in a database
  - **Email:** timely & securely correspond with other US BICES-X Users
  - **Voice/VTC**: seamless, immediately and personal

Demonstration of Tools

Demonstration of Tools

- Demonstration of various US BICES-X tools
  - **SYSTRAN** translation tool
  - **Shared Folders**: private folders versus public folders
  - **Product Library**: conducting a search and review meta tags
  - **Email:** personal versus group
  - **Voice/VTC**: how to conduct a VTC and share desktop
  - Mapviz

Demonstration of Tools

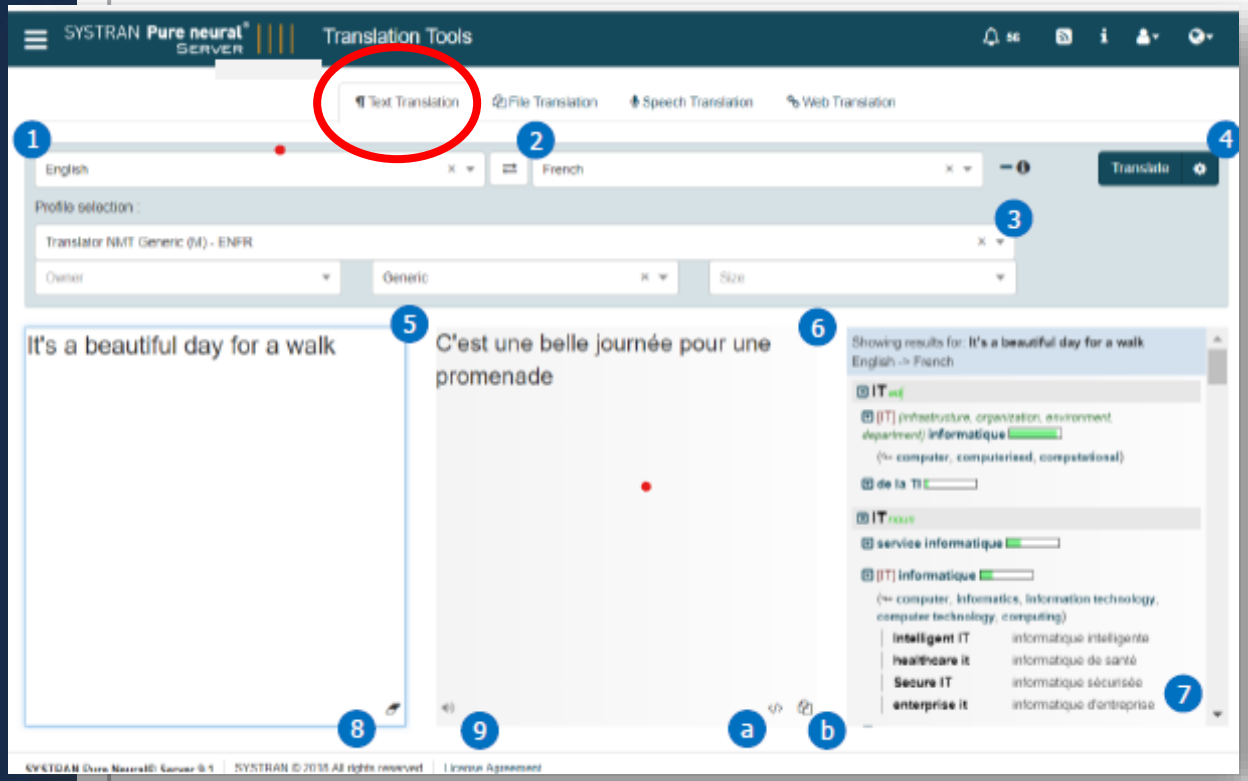
(SYSTRAN Translation Tool)

SYSTRAN Translation Tool

- Web translation capability for text and files

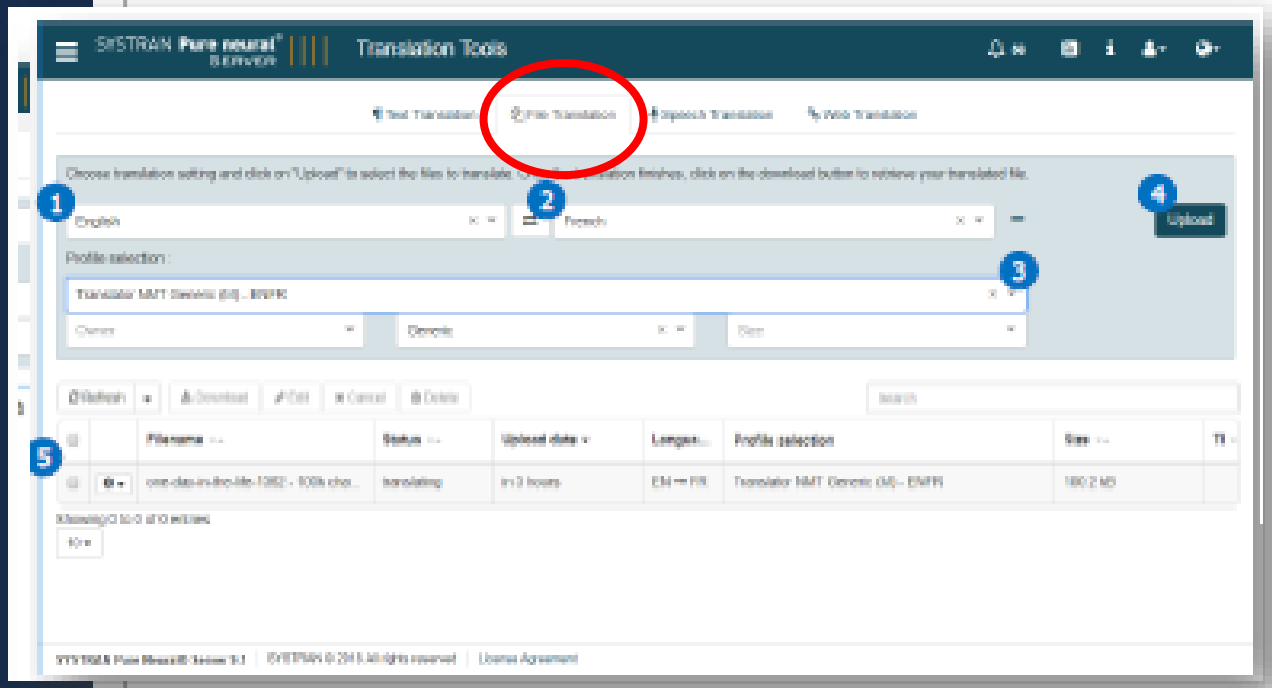
SYSTRAN
beyond language

SYSTRAN Text Translation



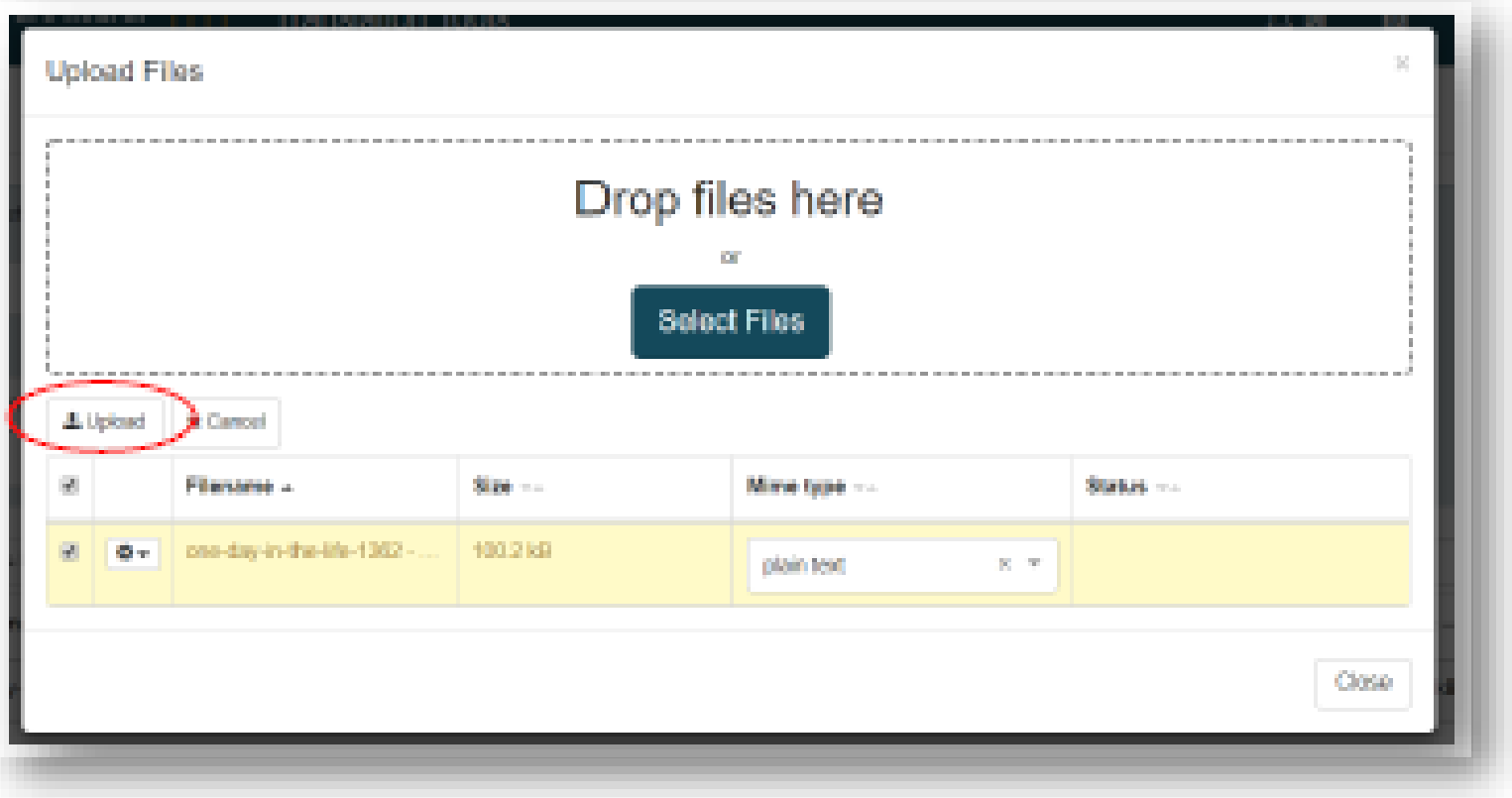
1.Source Language
2.Target Language
3.Profile selection
4.Translation format options
5.Text input field
6.Translation output
7.Terminology lookup panel
8.Erase text
9.Audio Translation (some browsers)
a.Copy html to clipboard
b.Copy translation to clipboard

File Translation



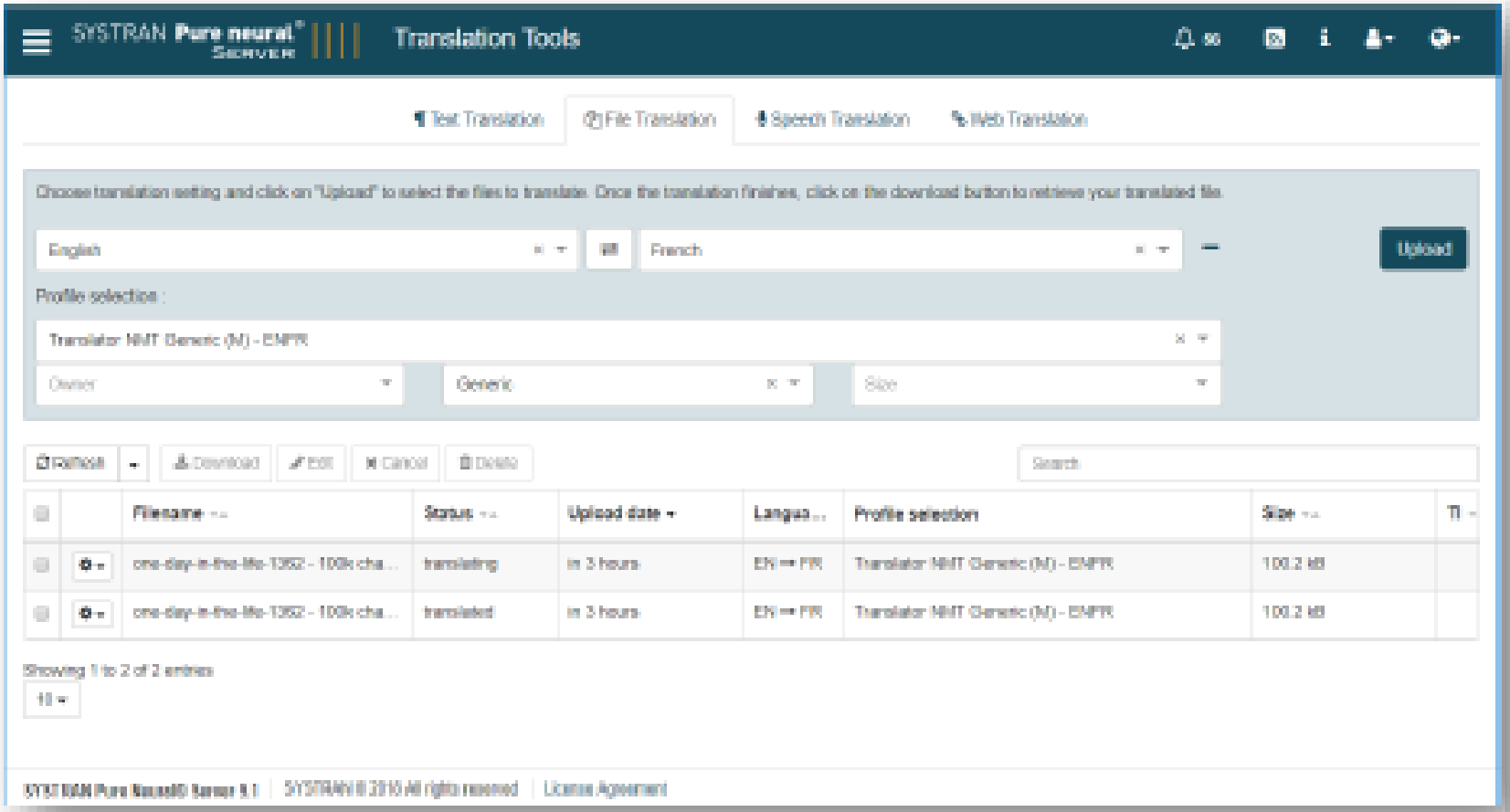
1.Source Language
2.Target Language
3.Profile selection
4.Upload Files
5.Translated file list currently existing on the server

File Translation – *Upload Files*



Drag and drop file, or select the file from File Explorer and upload

File Translation – *View Translations*



Track status, select to view

Demonstration of Tools

(Shared Folders)

Shared Folders Highlights

- Public Folders
  - All users have read/write access
- Private Folders
  - Users with access to private folders have read/write access
  - Permissions assigned by organization
    - Organization based off DD2875 request form

Demonstration of Tools

(Product Library)

Product Library Highlights

- Searchable repository hosting intelligence products
- Intelligence is tagged, uploaded and managed by the CDC-P
- Possible Search Functions
  - By Keyword
  - By Category
  - By Date
  - By Classification etc.

Demonstration of Tools

(Outlook Email)

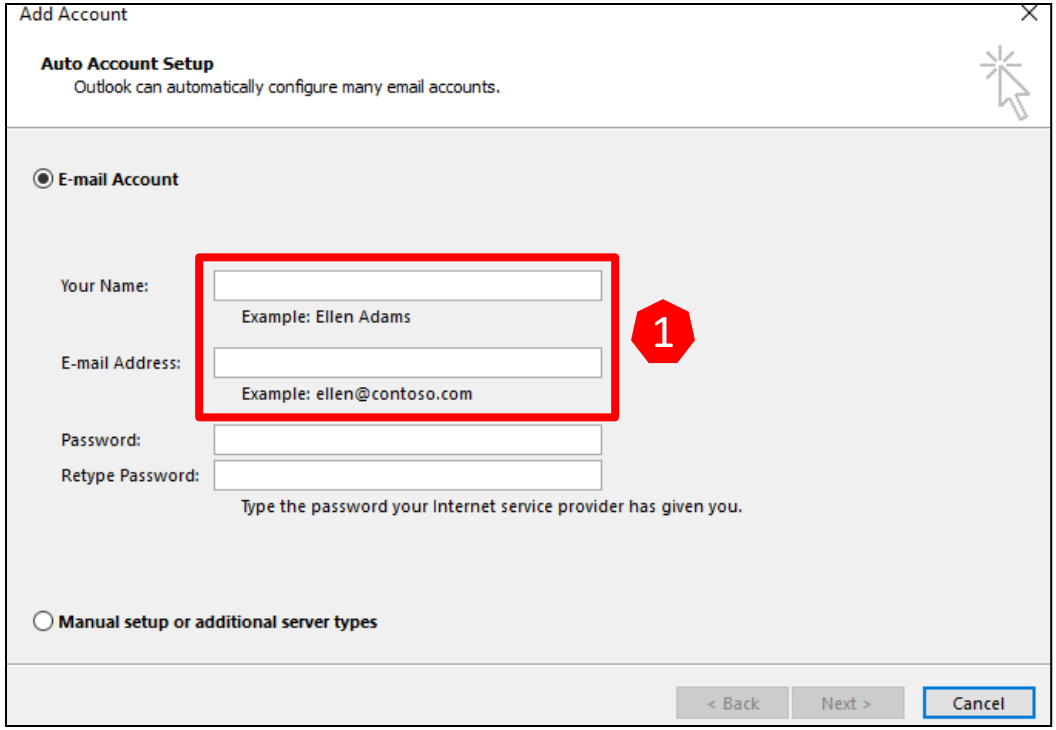
Email Highlights

- Provides secure e-mail between users on US BICES-X
- Accredited up to the SECRET RELEASEABLE level
- Outlook Directory to search for users on US BICES-X

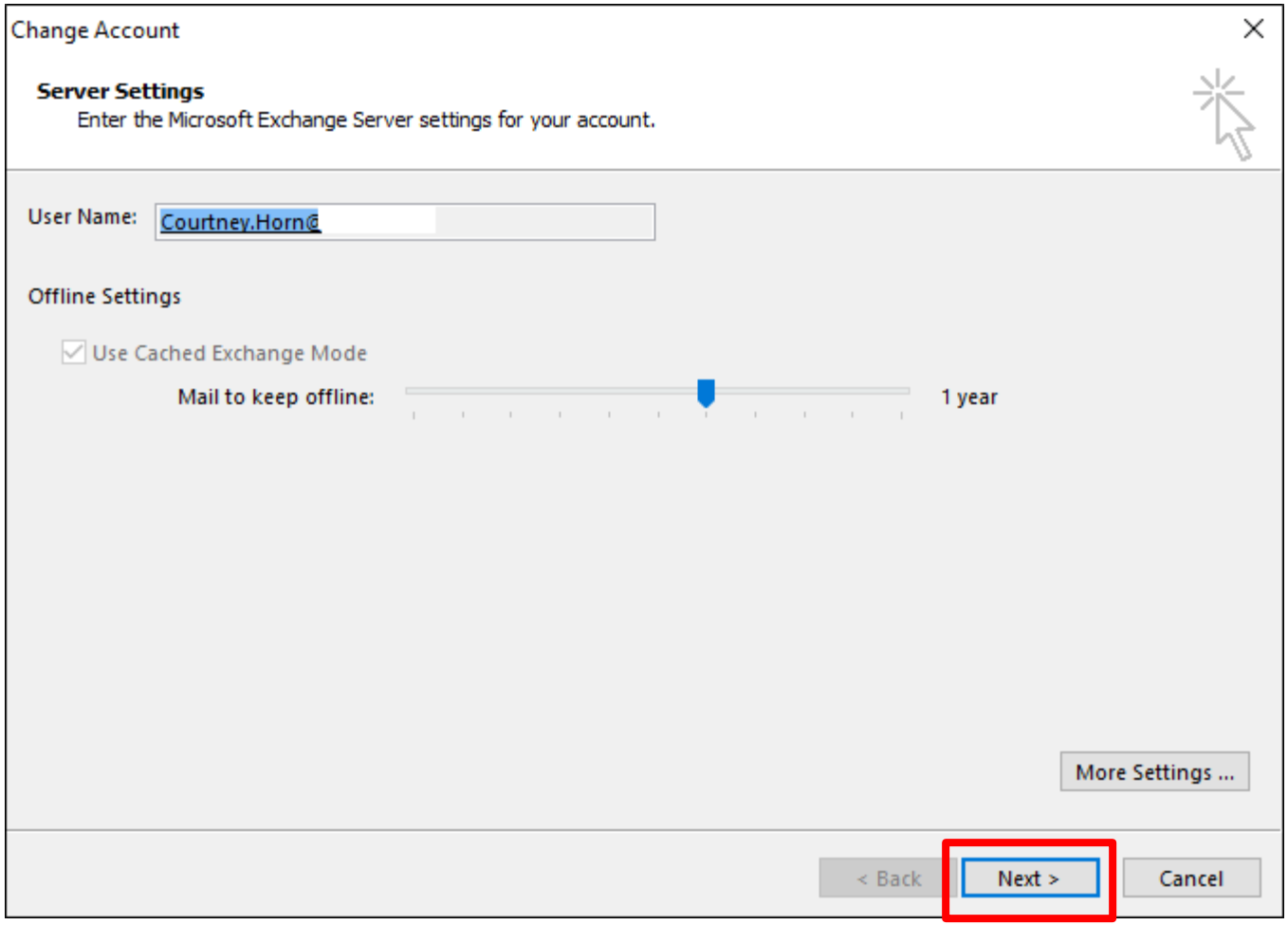
Email Outlook First time setup

- Launch Microsoft Office 2016

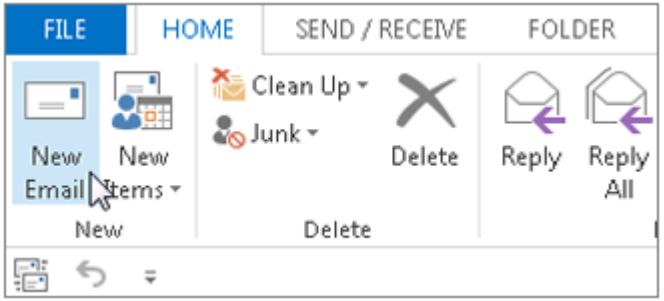
- The Name and Email Address field will auto populate 1



Email Outlook First time setup



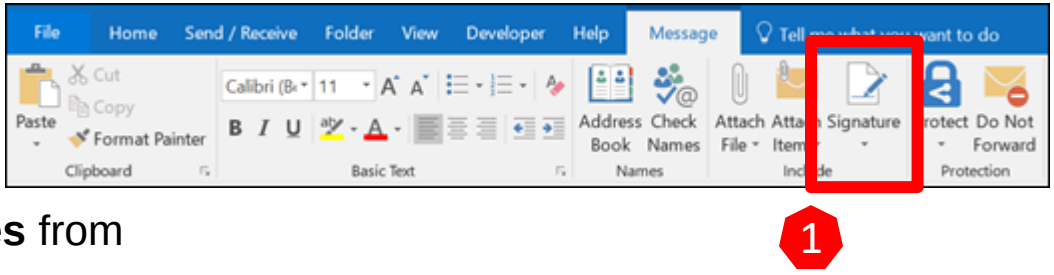
Sending Emails

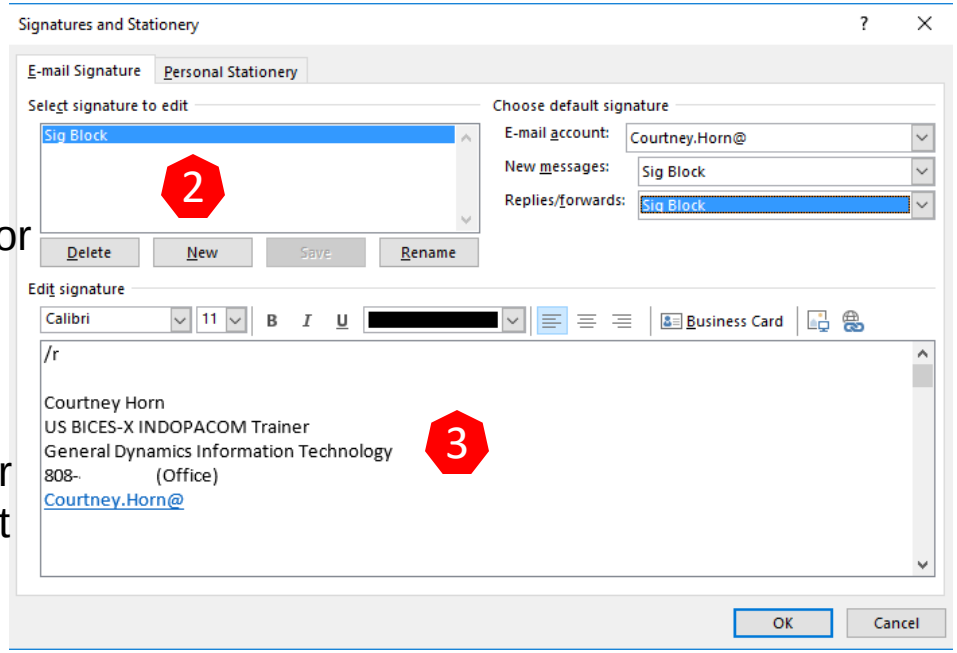


- Select “New Email” 1
- Select corresponding Classification
- Add select/type intended recipients
- Complete Subject and Body
- Send
- Remember to send emails in “PLAIN TEXT” not “HTML” format

Signature Block

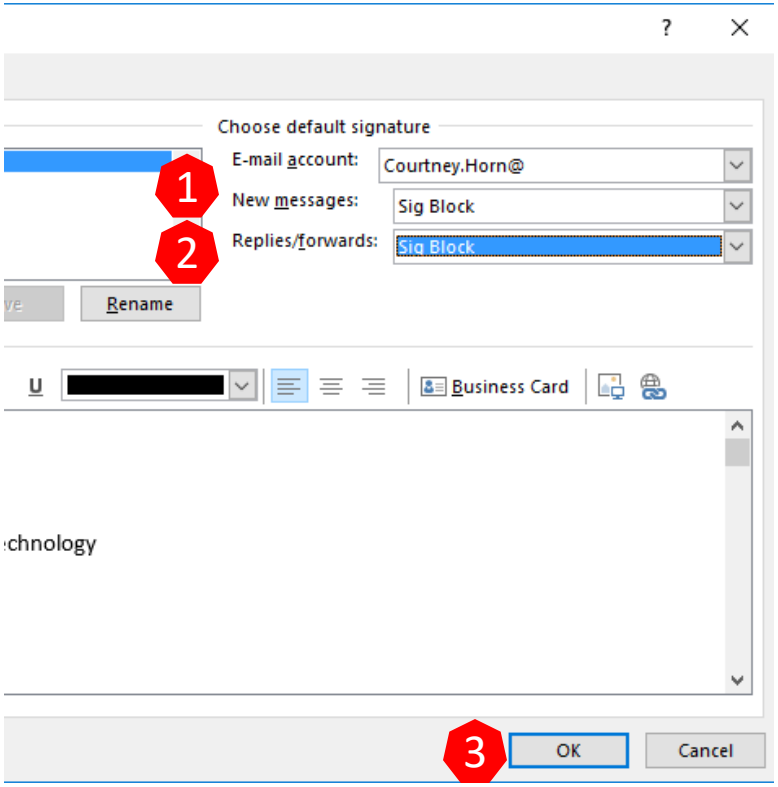
- Open a new email message.
- Select **Signature** > **Signatures** from the **Message** menu. 1
- Under **Select signature to edit**, choose **New**, and in the **New Signature** dialog box, type a *name* for the signature. 2
- Under **Edit signature**, compose your signature. You can change fonts, font colors, and sizes, as well as text alignment. Create the signature into the **Edit signature** box. 3





Signature Block

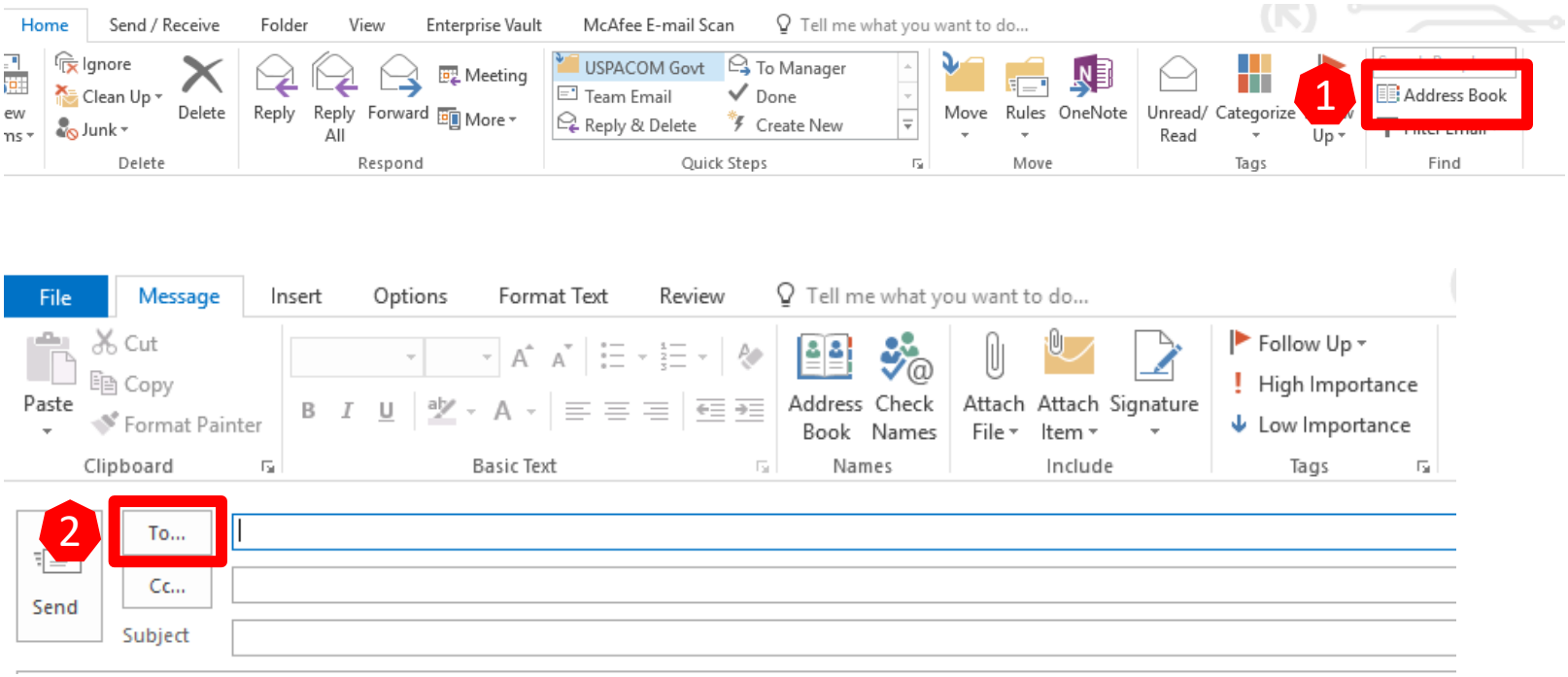
- If you want your signature added to all new messages by default, in the **New messages** drop-down box, select one of your signatures. 1
- If you want your signature to appear in the messages you reply to and forward, in the **Replies/forwards** drop-down, select one of your signatures. Otherwise, accept the default option of (none). 2
- Choose **OK** to save your new signature and return to your message. 3



Address Book

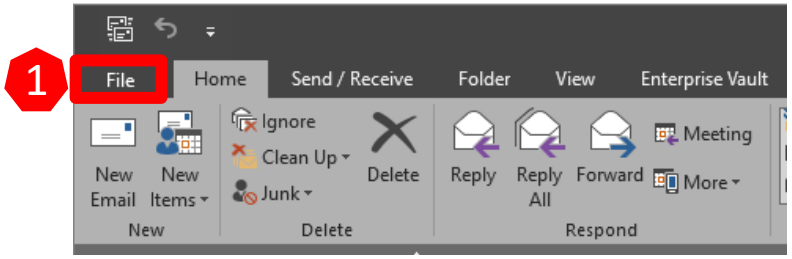
- Repository of all users that is searchable and displays contact information

- Click **Address Book** 1 or on a new email select **To** 2



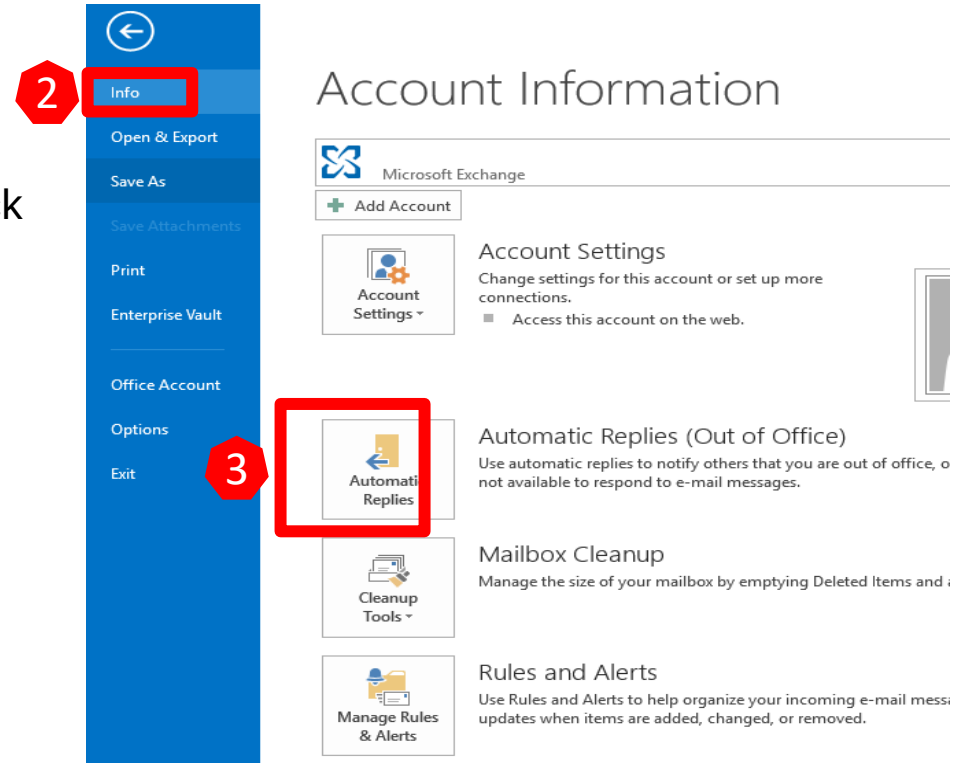
Automatic Replies

- Auto replies can be used for multiple reasons, these may include being out of the office or simply to inform the sender of an alternate communication method.



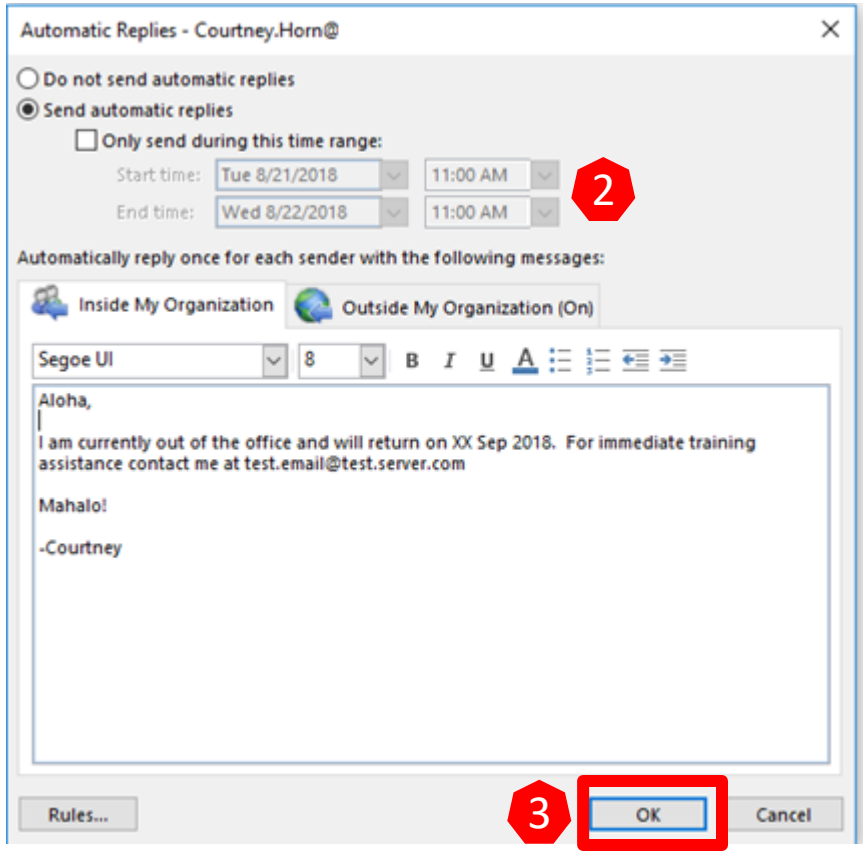
- Click the **File** 1 tab, and then click the **Info** 2 tab in the menu.

- Click **Automatic Replies (Out of Office)**. 3



Automatic Replies

- In the **Automatic Replies** dialog box, select the **Send Automatic Replies** check box. 1
- If you want to specify a set time and date range, select the **Only send during this time range** check box. Then set the **Start time**, and then set the End time. 2
- Draft Auto response and select **OK** 3



Demonstration of Tools

(Voice / VTC)

Voice/VTC Capability Highlights

- Provides a secure voice or video teleconferencing capability between two or more parties on US BICES-X
- US BICES-X account **NOT REQUIRED** for use
- Accredited up to the SECRET RELEASEABLE level
- Directory displays system locations on the network

Voice/VTC Capabilities

Before Calling

- Ensure that the room is secure
- Place a sign outside the closed door indicating a secure VTC
- Confirm that the room classification is appropriate for meeting
- Certify the VTC camera and microphone are not providing a view of any unrelated classified materials or unrelated classified discussions
- Turn on or off camera or microphone, as appropriate

Making a Call

- Demonstration of initiating a call
- Upon connection, announce classification of VTC
- Secure area for classification of call

Conference Lines
(Voice / VTC)

Creating a Conference

- One-time conference bridge vs standing (multi-use) conference bridges
- One-time or standing bridge created by contacting the Service Center West Help Desk
  - Contact details for Service Center located at the end of this presentation

US BICES-X Accounts

US BICES-X Account Request

- Requirements to obtain an US BICES-X User account:
  - DoD Annual Cyber Awareness Training Certificate
  - DD Form 2875, SAAR System Authorization Access Request
  - DD Form 2875 Addendum, Acceptable Use Policy
- Personnel requiring an account must be cleared to the SECRET RELEASABLE level

US BICES-X Account Request

- System Authorization Access Request (SAAR) DD FORM 2875 and US BICES-X Addendum
- User to complete **YELLOW** highlighted portions
- Supervisor to complete **GREEN** highlighted for initial approval

SYSTEM AUTHORIZATION ACCESS REQUEST (SAAR)

PRIVACY ACT STATEMENT

AUTHORITY: Executive Order 10450, 9397; and Public Law 99-474, the Computer Fraud and Abuse Act.
PRINCIPAL PURPOSE: To record names, signatures, and other identifiers for the purpose of validating the trustworthiness of individuals requesting access to Department of Defense (DoD) systems and information. NOTE: Records may be maintained in both electronic and/or paper form.
ROUTINE USES: None.
DISCLOSURE: Disclosure of this information is voluntary; however, failure to provide the requested information may impede, delay or prevent further processing of this request.

TYPE OF REQUEST: [X] INITIAL [ ] MODIFICATION [ ] DEACTIVATE [ ] USER ID _____ | DATE (YYYYMMDD)

SYSTEM NAME (Platform or Applications): US BICES-X (APIIN) | LOCATION (Physical Location of System)

PART I (To be completed by Requestor)

1. NAME (Last, First, Middle Initial)	2. ORGANIZATION	
3. OFFICE SYMBOL/DEPARTMENT	4. PHONE (DSN or Commercial)	
5. OFFICIAL E-MAIL ADDRESS	6. JOB TITLE AND GRADE/RANK	
7. OFFICIAL MAILING ADDRESS	8. CITIZENSHIP [ ] US [X] FN [ ] OTHER	9. DESIGNATION OF PERSON [X] MILITARY [ ] CIVILIAN [ ] CONTRACTOR

10. IA TRAINING AND AWARENESS CERTIFICATION REQUIREMENTS (Complete as required for user or functional level access.)
[ ] I have completed Annual Information Awareness Training. DATE (YYYYMMDD) _____

11. USER SIGNATURE | 12. DATE (YYYYMMDD)

PART II - ENDORSEMENT OF ACCESS BY INFORMATION OWNER, USER SUPERVISOR OR GOVERNMENT SPONSOR (If individual is a contractor - provide company name, contract number, and date of contract expiration in Block 16.)

13. JUSTIFICATION FOR ACCESS
Mission Requirement

14. TYPE OF ACCESS REQUIRED: [X] AUTHORIZED [ ] PRIVILEGED

15. USER REQUIRES ACCESS TO: [ ] UNCLASSIFIED [X] CLASSIFIED (Specify category) APIIN [ ] OTHER _____

16. VERIFICATION OF NEED TO KNOW
I certify that this user requires access as requested. [X]
16a. ACCESS EXPIRATION DATE (Contractors must specify Company Name, Contract Number, Expiration Date. Use Block 27 if needed.)

17. SUPERVISOR'S NAME (Print Name)	18. SUPERVISOR'S SIGNATURE	19. DATE (YYYYMMDD)
20. SUPERVISOR'S ORGANIZATION/DEPARTMENT	20a. SUPERVISOR'S E-MAIL ADDRESS	20b. PHONE NUMBER
21. SIGNATURE OF INFORMATION OWNER/OPR	21a. PHONE NUMBER	21b. DATE (YYYYMMDD)
22. SIGNATURE OF IAO OR APPOINTEE	23. ORGANIZATION/DEPARTMENT	24. PHONE NUMBER / 25. DATE (YYYYMMDD)

DD FORM 2875, AUG 2009 PREVIOUS EDITION IS OBSOLETE. Adobe Professional 8.0

US BICES-X Account Request

- User complete **Section 26**
- Review and Complete US BICES-X Addendum (later slide)
- Partner appointed Security Manager to complete **BLUE** highlighted “Part III”

26. NAME *(Last, First, Middle Initial)*			
27. OPTIONAL INFORMATION *(Additional information)*			
PART III - SECURITY MANAGER VALIDATES THE BACKGROUND INVESTIGATION OR CLEARANCE INFORMATION			
28. TYPE OF INVESTIGATION		28a. DATE OF INVESTIGATION *(YYYYMMDD)*	
28b. CLEARANCE LEVEL		28c. IT LEVEL DESIGNATION ☐ LEVEL I ☐ LEVEL II ☒ LEVEL III	
29. VERIFIED BY *(Print name)*	30. SECURITY MANAGER TELEPHONE NUMBER	31. SECURITY MANAGER SIGNATURE	32. DATE *(YYYYMMDD)*
PART IV - COMPLETION BY AUTHORIZED STAFF PREPARING ACCOUNT INFORMATION			
TITLE:	SYSTEM	ACCOUNT CODE	
	DOMAIN		
	SERVER		
	APPLICATION		
	DIRECTORIES		
	FILES		
	DATASETS		
DATE PROCESSED *(YYYYMMDD)*	PROCESSED BY *(Print name and sign)*	DATE *(YYYYMMDD)*	
DATE REVALIDATED *(YYYYMMDD)*	REVALIDATED BY *(Print name and sign)*	DATE *(YYYYMMDD)*	

DD FORM 2875 (BACK), AUG 2009 Reset

US BICES-X Account Request

DD2875 Addendum
APIIN Acceptable Use Policy

The Office of Management and Budget (OMB) Circular A-130, Appendix III, "Security of Federal Automated Information Resources" requires that an "Acceptable Use Policy" be established on each information technology (IT) system that processes government information. The "Acceptable Use Policy" delineated below pertains to all persons who access the Asia/Pacific Intelligence Information Network (APIIN) resources resident in the PACOM Area of Responsibility.

As a user of PACOM's APIIN resources, I understand that I am responsible for adhering to the rules listed below:

1. Computer system(s) for which you are requesting or have been issued an account may only be used for official missions and DoD-supported missions.

2. All software on the IT resource is protected in accordance with Federal Government security and control procedures.

3. Use of these IT resources gives consent for monitoring and security testing to ensure proper security procedures and appropriate usage.

4. APIIN IT resources will not be used for fraudulent, harassing or obscene messages and/or materials.

5. Tampering with another user's account, files, data or processes without the other user's express permission, use of the system resources for personal purposes, or other unauthorized activities is strictly prohibited and will result in termination of access privileges.

6. Usernames and passwords may never be transferred or shared for any reason.

7. Group ID and passwords are prohibited. Organizations that wish to sponsor "watch accounts" will have a common mailbox (e.g. "Watch.Organization@..." email address) attached to individual accounts.

8. Passwords:
   a. will be a minimum of 14 characters;
   b. will include at least two each: numbers, upper/lower case letters, special characters
   c. will be memorized and not written down;
   d. will be changed at least every 60 days;
   e. will not be a word appearing in an English or foreign dictionary;
   f. will not be stored in keyboard macros, script, or batch files;
   g. will not consist of personal ID data or be easily guessable;
   h. will not reuse the same password within a 180 day period;
   i will have cycled through 24 passwords before reuse.

9. E-mail and other forms of electronic distribution will only be used for official purposes and will not be used to transmit information that is not releasable to the clearance level, need-to-know and or classification of the network.

10. Tampering or reverse engineering of the IT resource is prohibited.

11. All media introduced to the system will be virus scanned prior to introduction to any systems.

12. No modifications will be made to the system without prior approval of the APIIN Information Assurance Manager.

13. Uploading un-authorized software or a deviation from the current software baseline is strictly prohibited and may result account lockout, loss of privilege to system and notification to local

US BICES-X Account Request

- User to complete all **YELLOW** highlighted section
- Security Manager or User to complete **BLUE** Clearance/Date
  - Reference “Part III”

DD2875 Addendum
APIIN Acceptable Use Policy

security staff for further investigation.

14. Any unauthorized penetration attempt, unauthorized system use, or virus activity will be reported to your supervisor, system administrator, IS Security Officer and the DAA.

15. When access is no longer required to these IT resources, notify appropriate responsible parties to terminate access and make no further attempt to access these resources. An account will be considered “abandoned” after 90 days of inactivity and will be disabled; after 120 days of inactivity, it will be deleted.

16. Failure to adhere to these rules or subvert these rules may constitute grounds for termination of access privileges, administrative action, and/or civil or criminal prosecution.

17. All incidents or suspected incidents should be reported to your local APIIN support staff or security representatives.

18. Any system used to connect either directly or remotely to the APIIN network(s) must be approved in advance by the DAA.

19. VOIP Phones will be used only to pass communications for official purposes that are relative to the need to know, classification and approval of the APIIN data owner or program office.

Acknowledgement Statement

Unauthorized use of the computer accounts and computer resources to which I am granted access is a violation of Section 799, Title 18, U.S. Code; constitutes theft; and is punishable by law. I understand that I am the only individual to access these accounts and will not knowingly permit access by others without written approval from the Security Manager.

I understand that my misuse of assigned accounts and my accessing others' accounts without authorization is prohibited. I understand that this/these system(s) and resources are subject to monitoring and recording. I further understand that failure to abide by these provisions may constitute grounds for termination of access privileges, administrative action, and/or civil or criminal prosecution.

Date:	Name (Print):	Signature:
Phone:	Organization:	Unclassified email address:
Citizenship of Requestor:	Level of Privilege: ☑ (User) ☐ (Developer) ☐ (Admin)	Clearance/Date:

US BICES-X Account Request

- Complete and sign all forms, validate by Supervisor and Security Manager and email forms to the following:
  - **apiin.bices-x.fct@pacom.mil**
- Account creation process may take up to 2 weeks
- Account Requirements
  - DoD Annual Cyber Awareness Training Certificate - (valid for one year from date of issuance)
  - DD Form 2875, SAAR – System Authorization Access Request
  - DD Form 2875 Addendum, Acceptable Use Policy

User IDs and Passwords

- User IDs and passwords are individual identifiers whose purpose is to control access to the network and establish individual accountability

- Network users shall not:
  - Use any means other than their assigned user ID and password to access the network;
  - Divulge their network password to any other person;
  - Surrender physical control of an operational workstation without first logging off the workstation

Disposition of User IDs / Passwords

- A user's account will be disabled when:
  - A user no longer requires access to the network;
  - DoD Annual Cyber Awareness Training Certificate has expired – valid for one year from date of issuance;
  - The user's account has not been utilized for over 30 days

Service Center West

Service Center West Help Desk

- Assist with day-to-day operations
  - Account assistance (Creation, Unlock, Password Reset)
  - General troubleshooting
  - VTC technical assistance
  - Shared Folder Creation

- US BICES-X Network: 0000
- Commercial Phone: +1 808 477-8105
- apiin.bices-x.fct@pacom.mil (UNCLASS)
- Support@XXX.cmil.mil

Hours of Operation:

Local Time Tuesday – Saturday: **0000-1200**

HST Monday – Friday: **0600-1800**

Contact Information

Service Center West Help Desk

US BICES-X VoIP: 0000

Commercial Phone: +1 808 473-8105

Unclass Email: apiin.bices-x.fct@pacom.mil

US BICES-X Email: Support@XXX.cmil.mil

Consolidated Dissemination Center – Pacific

US BICES-X VoIP: 0063880

Commercial Phone: +1 808 473-6062

Unclass Email: CDCP_analyst@dodiis.mil

US BICES-X Email: CDCP_analyst@***.cmil.mil


US BICES-EXTENDED ENTERPRISE
US BICES-X

Questions?


U.S. INDO-PACIFIC COMMAND