

Trusted Network Environment (TNE)

OVERALL CLASSIFICATION: UNCLASSIFIED



CONNECTS THE COALITION

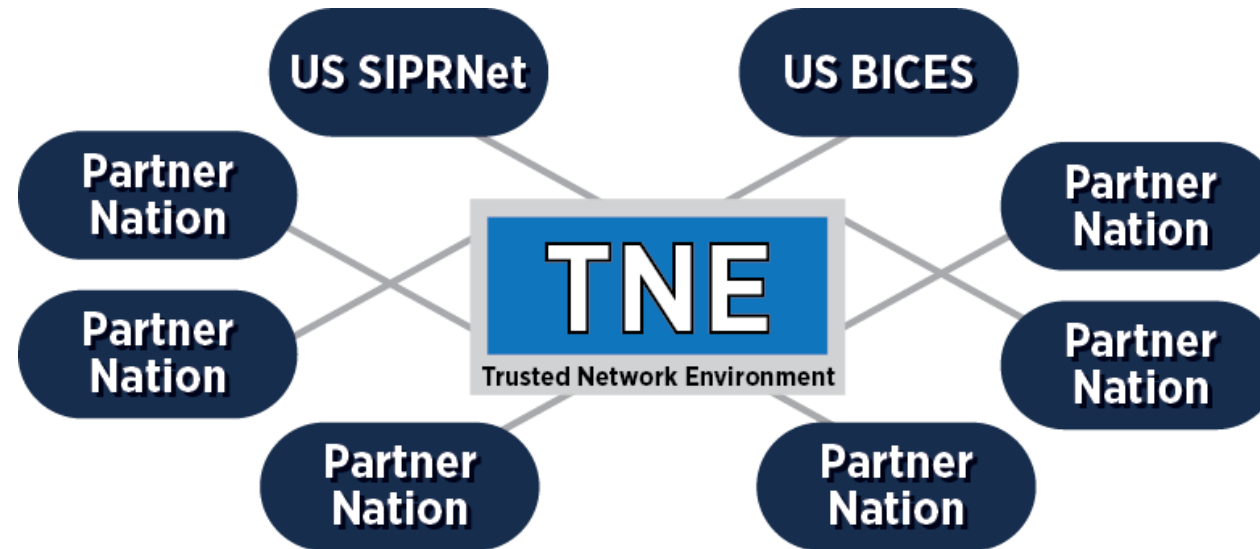


UNCLASSIFIED

Objective



Understand which services are offered through the Trusted Network Environment (TNE).



UNCLASSIFIED

US BICES-X Mission and Purpose



- The DoD requires an enduring, secure information sharing capability with partners around the world
- US BICES-eXtended extends US BICES S//REL services to the coalition mission partners of the Combatant Commands
- US BICES-eXtended is capable of bilateral and multinational communications and ensures the security and the releasable aspect of all information
- The Trusted Network Environment (TNE) is a cross-domain solution enabling US BICES-X and the sharing of information between multiple coalition partners



UNCLASSIFIED

Joint OUSD/I & DOD CIO memo 1 December 2014:

"US BICES/US BICES-X shall be the Department of Defense Coalition Intelligence Information Sharing enduring capability in support of coalition partners at the SECRET REL level. As MPE architectures and capabilities evolve, they may build upon US BICES/US BICES-X capabilities which could expand to address other coalition functions in the future."

UNCLASSIFIED

OFFICE OF THE SECRETARY OF DEFENSE
WASHINGTON, DC 20301-1000

DEC 01 2014

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
CHIEFS OF THE MILITARY SERVICES
COMMANDERS OF THE COMBATANT COMMANDS
DIRECTOR, COST ASSESSMENT AND PROGRAM EVALUATION
DIRECTORS OF DEFENSE AGENCIES
DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY

SUBJECT: Coalition Intelligence Information Sharing

Continuing and expanding requirements to share intelligence and collaborate with partner nations at the SECRET REL level has become vital to U.S. operations worldwide. These needs arise across the full spectrum military of operations, and include enhancing enduring partnerships as well as responding to emerging threats globally with new partner nations. US Battlefield Information, Collection, and Exploitation System (BICES) is currently the DoD enduring solution to provide this capability in support of the North Atlantic Treaty Organization and other designated partners. US BICES eXtended (US BICES-X) expands this capability globally in support of all Combatant Commands and efficiently share intelligence support to

US BICES-X aggregated intelligence rapidly deployable capabilities and the ability to support intelligence information enterprise. BICES-X is identified (MPE).

A challenge is DoD Components must services. To that end Intelligence Information

SECRET REL level. As MPE architectures and capabilities evolve, they may build upon US BICES/US BICES-X capabilities which could expand to address other coalition functions in the future.

USD(I) established the DIIIE Council as the primary governance body to shape investment decisions for the Intelligence Mission Area component of the DoD Information Enterprise Architecture. The DIIIE Council shall exercise oversight of US BICES/US BICES-X through the International Partners Action Group on behalf of USD(I) and DoD CIO; and include representatives from the Joint Staff, Combatant Commands, and Combat Support Agencies.

The point of contact for US BICES-X is Mr. Richard Radcliffe, Director, US BICES and International Intelligence Programs. He can be reached at (703) 604-1875. The point of contact for the DoD CIO is Mr. David Cotton, Deputy Chief Information Officer for Information Enterprise. He can be reached at (703) 695-0871.

Kory Halvorsen
DoD Chief Information Officer
(Acting)

Michael G. Vickers
Under Secretary of Defense
for Intelligence

UNCLASSIFIED
Classification for training purposes only.

What is US BICES-X

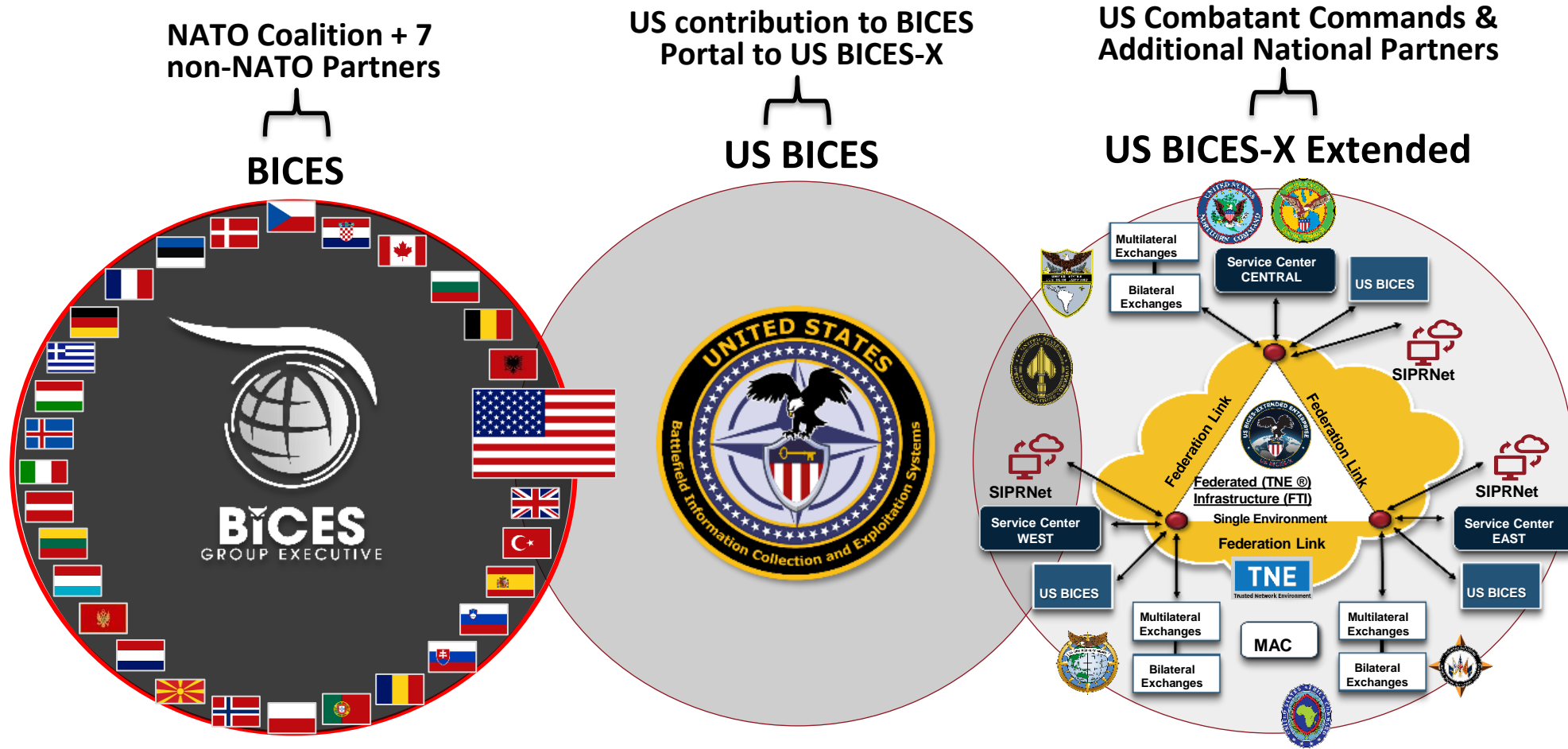


- US BICES-X is not a traditional network but rather, implements a sophisticated cross-domain solution that connects with multiple networks
- The United States and several partner networks are connected via US BICES-X:
 - US SIPRNet
 - United States Battlefield Information Collection and Exploitation Systems (US BICES) network (30 NATO countries seamlessly connected)
 - Various bilateral networks with partner nations and multilateral networks supporting COIs such as the maritime communities



UNCLASSIFIED

Flavors of BICES



The Battlefield Information Collection and Exploitation Systems (BICES) has three flavors: 1) BICES: NATO & 7 non-NATO coalition partners, 2) US BICES: US National Contribution into BICES, 3) US BICES-X: the extended version of US BICES to all Combatant Commands (CCMDs) and their coalition partners.



UNCLASSIFIED



- What is TNE?
- Account Request
- Email
- Voice over IP (VoIP) phone calls
- Chat
- Web/File Share
- Email and File Share Rejection Fixes
- Points of Contact



What is TNE?



- The Trusted Network Environment (TNE) is the cross- domain solution within US BICES-X that controls access to data sent via 4 services.
 1. Email
 2. Voice
 3. Chat
 4. Web/File Share
- Connects with other coalition networks through the **Domain Gateway (DG)**





UNCLASSIFIED



Account Requests

UNCLASSIFIED

- Required documents for TNE account
 - DoD Form 2875 Feb 2022
 - USBICES DoD Standard Mandatory Notice and Consent
 - Cyber Awareness Training Certificate
- Accessing TNE from SIPRNet or USBICES
 - Users must be authorized to handle NATO SECRET information
- Complete USBICES/TNE account request forms and send to the Coalition Support Service Desk (CSSD)
 - (UNCLASS) osd.molesworth.osd.mbx.usbices-coalition-service-desk@mail.mil
 - (SIPR) osd.molesworth.osd.mbx.usbices-coalition-service-desk@smil.mail.mil
 - (USBICES) osd.molesworth.osd.mbx.usbices-coalition-service-desk@mail.mil

User Category for Web Accounts



- Web Accounts
 - **Category 1**
 - Upload/Relabel/Download
 - **Category 2**
 - Upload/Download
 - **Category 3**
 - Download
 - This is the category requested as part of the user form when requesting a TNE account
 - Typically, users have a Category 1 account



UNCLASSIFIED

TNE Account Request Forms



//UNCLASSIFIED//

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		DATE (YYYYMMDD)	
<input type="checkbox"/> INITIAL <input type="checkbox"/> MODIFICATION <input type="checkbox"/> DEACTIVATE <input type="checkbox"/> USER ID			
SYSTEM NAME (Platform or Application)		LOCATION or SITE ID	
<input type="checkbox"/> US BICES <input type="checkbox"/> TNE		OTHER EX. RAF Molesworth / Site 100	
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 EX. GS15/CIV or O4/MAJ or CTR	
7. OFFICIAL MAILING ADDRESS		8. NATIONALITY / AFFILIATION	
		<input type="checkbox"/> US <input type="checkbox"/> 7 NNN <input type="checkbox"/> MILITARY <input type="checkbox"/> CIVILIAN <input type="checkbox"/> NATO <input type="checkbox"/> SVN <input type="checkbox"/> CONTRACTOR	
9. DESIGNATION OF PERSON			
10. IA TRAINING AND AWARENESS CERTIFICATION REQUIREMENTS (Complete as required for user or functional level access.)			
<input checked="" type="checkbox"/> 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 18.)			
13. JUSTIFICATION FOR ACCESS			
The account requestor's supervisor (or US sponsor if requestor is a foreign national) will sign block 18 asserting that:			
The above individual has valid need to know and operational requirement for access to US BICES-X information. Additionally, the user will sign and submit the Consent to Monitoring/Acceptable Use Policy along with this form.			
Privilege Account Type: (WS, SA, DA, NA, etc.)			
Job Title:			
Duties and Detailed Justification for Elevated Privileges:			
14. TYPE OF ACCESS REQUIRED:			
<input checked="" type="checkbox"/> AUTHORIZED <input type="checkbox"/> PRIVILEGED			
15. USER REQUIRES ACCESS TO: <input type="checkbox"/> UNCLASSIFIED <input type="checkbox"/> CLASSIFIED (Specify category) SECRET Releasable			
<input type="checkbox"/> OTHER			
16. VERIFICATION OF NEED TO KNOW		16a. ACCESS EXPIRATION DATE (Contractors must specify Company Name, Contract Number, Expiration Date. Use Block 27 if needed.)	
I certify that this user requires access as requested. <input checked="" type="checkbox"/>			
17. SUPERVISOR'S NAME (Print Name)		18. SUPERVISOR'S SIGNATURE	
LAST, FIRST, MI.			
20. SUPERVISOR'S ORGANIZATION/DEPARTMENT		20a. SUPERVISOR'S E-MAIL ADDRESS	
		20b. PHONE NUMBER	
21. SIGNATURE OF INFORMATION OWNER/OPR		21a. PHONE NUMBER	
Not Applicable (see block 18)		Not Applicable (see block 20b)	
22. SIGNATURE OF TAO, SSO, Unit Security Manager		21b. DATE (YYYYMMDD)	
		Not Applicable	
23. ORGANIZATION/DEPARTMENT		24. PHONE NUMBER	
		25. DATE (YYMMDD)	

DD FORM 2875, AUG 2009 PREVIOUS EDITION IS OBSOLETE. Advice Designer 5.0

//UNCLASSIFIED//

//UNCLASSIFIED//

26. NAME (Last, First, Middle Initial)			
LAST, FIRST, MI.			
27. OPTIONAL INFORMATION (Additional information)			
TNE User Category			
-- Signed Acceptable Use Policy (AUP): <input type="checkbox"/> YES <input type="checkbox"/> NO			
<input type="checkbox"/> 1 - Read/Write/Re-label (e.g. FDOs, managers)			
<input type="checkbox"/> 2 - Read/Write (e.g. analysts)			
<input type="checkbox"/> 3 - Read only (e.g. data consumers)			
Network TNE is accessed from:			
If the network is sensitive, this form must be protected as appropriate.			

Unit Security Manager or SSO must complete and sign part III verifying security clearance level of user.			

Additional Required Information to process accounts within US BICES-X			
* FDO Completion Date:			
* Must be a IT Level I or II with a SSB/SPR/PPR/T5 type of investigation			
* US BICES-X Information Technology Acceptable Use and User Agreement			
* DoD Cyber Awareness Challenge Certificate (Completed within 1 Year)			
* Appointment Orders for assigned position (to be signed by US BICES ISSM)			
* Privileged Level Access Agreement (PLAA) & Acknowledgment of Responsibilities			
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	
		<input type="checkbox"/> LEVEL I <input type="checkbox"/> LEVEL II <input type="checkbox"/> 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:		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

//UNCLASSIFIED//

Be sure to identify which network you will be logging in from (i.e. SIPR, US BICES, etc.)



UNCLASSIFIED

TNE Account Request Forms



UNCLASSIFIED



US BICES-X United States Battlefield Information
Collection and Exploitation Systems-
Extended

DoD STANDARD MANDATORY NOTICE AND CONSENT

By signing this document, you acknowledge and consent that when you access Department of Defense (DOD) information systems:

1. You are accessing a U.S. Government (USG) information system (IS) (which includes any device attached to this information system) that is provided for U.S. Government authorized use only.
2. You consent to the following conditions:
 - a. I understand the U.S. Government routinely intercepts and monitors communications on this information system for purposes including, but not limited to, penetration testing, communications security (COMSEC) monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.
 - b. I understand that at any time, the U.S. Government may inspect and seize data stored on this information system (IS). This includes, but is not limited to user e-mails and instant messages exchanged on this IS.
 - c. I understand that communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any U.S. Government authorized purpose.
 - d. I understand this information system includes security measures (e.g., authentication and access controls) to protect U.S. Government interests not for my personal benefit or privacy.
 - e. Notwithstanding the above, using a US BICES-X information system constitutes consent to personnel misconduct, law enforcement, or counterintelligence investigative searching or monitoring. Declaration of privileged communications or data (including work product) that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants will be considered on a case by case basis. Under these circumstances, such communications and work product are private and confidential, as further explained below:
 - (1) Nothing in this User Agreement shall be interpreted to limit the user's consent to, or in any other way restrict or affect, any U.S. Government actions for purposes of network administration, operation, protection, or defense, or for

UNCLASSIFIED

UNCLASSIFIED

- s. I understand that monitoring of US BICES-X Information Systems will be conducted for various purposes and information captured during monitoring may be used for administrative or disciplinary actions or for criminal prosecution.
6. Acknowledgement. I have read the above requirements regarding use of US BICES-X systems, networks, and devices. I understand my responsibilities and liability regarding use of such systems and the safeguarding of information contained therein. I am subject to disciplinary action for violation of DOD, USAF, or US BICES policies. If I fail to comply, I am subject to adverse administrative action or punishment under Article 92 of the Uniform Code of Military Justice (UCMJ). If I am not subject to the UCMJ, I may be subject to administrative, disciplinary, or adverse action and/or civil or criminal prosecution for failing to comply with this agreement and/or DoD, USAF, US BICES policies for the use of DoD information systems.

Last Name:

First Name:

Middle Initial:

Rank/Grade: Ex. GG15

Signature:

Date/Time:



UNCLASSIFIED



Email

UNCLASSIFIED



- No cross-domain Global Address List (GAL) in Outlook
- Plain text (No HTML)
- No encrypted email
- No digital signatures
- Emails and attachments must have proper classification line with exact syntax
- Must have a policy in the TNE12S for classification line
- No dirty words
- An email can be sent to multiple recipients, on multiple domains





- Microsoft Outlook is typically provided to all TNE users who use their network provided workstations
- No Global Address List (GAL) in Outlook
 - TNE provides a web interface with contact information of TNE users
 - Users on country network workstation (not on SIPR or US BICES) will show users in their country
- TNE does not support “read receipt” requests or meeting notices
- No digital signatures
- No encryption



Email & Attachment Format: The Basics

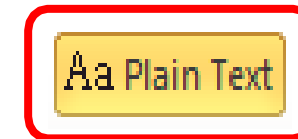


- Contain a classification and caveats text line above the body of the message:

Send To...
Cc...
Subject:

CLASSIFICATION: UNCLASSIFIED//REL TO USA, ###
(U//REL TO USA, ###) Body of Email goes here.
CLASSIFICATION: UNCLASSIFIED//REL TO USA, ###

- Formatted in plain text vs. html:



vs.



- Sending an email with an attachment through Outlook has file size limitations as high as 250MB. Based on your networks exchange server restrictions, the size limit could be smaller.



UNCLASSIFIED

Email Classifications



- All messages must contain a classification and caveat identifier at the top
- Examples of classifications for TNE messages:
 - **UNCLASSIFIED//REL TO USA, XXX**
 - **CONFIDENTIAL//REL TO USA, XXX**
 - **SECRET//REL TO USA, XXX**
 - **CUI//REL TO USA, XXX**
- All classifications require a REL caveat. Straight Unclassified, Confidential, or Secret are not authorized.
- The classification and caveat must be preceded by “Classification:” as in: Classification: SECRET//REL TO USA, XXX
- Classification Tool:
 - Most TNE users will have a tool (i.e. TITUS)
 - If none are available; type the classification and caveat

UNCLASSIFIED
Classification for training purposes only.

Please Choose a Classification -

Please select Classification level(s)

Classification

UNCLASSIFIED

*Unclass Caveat

Please Select

Please Select

NONE

FOR OFFICIAL USE ONLY

REL TO USA,

REL TO USA,

REL TO USA,

REL TO USA,

REL TO USA,

REL TO USA,

REL TO USA,

REL TO USA,

REL TO USA,

REL TO USA,



UNCLASSIFIED

Classifications leading with “//” like:

“CLASSIFICATION: //JOINT SECRET YYY USA//REL TO USA, YYY”

UNCLASSIFIED
Classification for training purposes only.

will work only if installed per the security policy. Contact your TNE12S Representative for a complete list of security labels.

- Authorized file types:
 - Word Processing: .doc .docm .docx
 - Spreadsheets: .xls .xlsm .xlsx
 - PowerPoint: .pps .ppsm .ppsx .ppt .pptm .pptx
 - Archives: .bz .bz2 .gz .tar .zip
 - Text-based: .csv .log .txt .xml
 - Graphics: .apm .bmp .dib .dws .emf .gif .j2c .j2k .jfi .jfif .jif .jp2 .jpc .jpe .jpeg .jpf .jpg .jpg2 .jpx .png .tif .tiff .wmf
 - Portable Documents: .pdf

Email Troubleshooting



- Most email issues are related to a missing or invalid classification. Keep in mind local network, mail classification tools may include classifications that are not authorized for use in the TNE
- Classifications are authorized and defined by the sharing matrix policy
- New classifications can be requested by users by submitting a new requirement to their local LNO



UNCLASSIFIED

- Refresher
 - Syntax of classification line still must be exact
 - Plain text (No HTML)
 - No encrypted email
 - No signed email
 - No email w/o classification line
 - Must have a policy in TNE12S for the classification line
 - Dirty word filter still in place
 - An email can still be sent to multiple recipients, on multiple domains



VoIP

UNCLASSIFIED

- This presentation is intended for users of the TNE 12S VoIP Infrastructure
- Contents
 1. VoIP Architecture Overview
 2. Making / Receiving a Call
 3. Dialing Plan
 4. Current Limitations

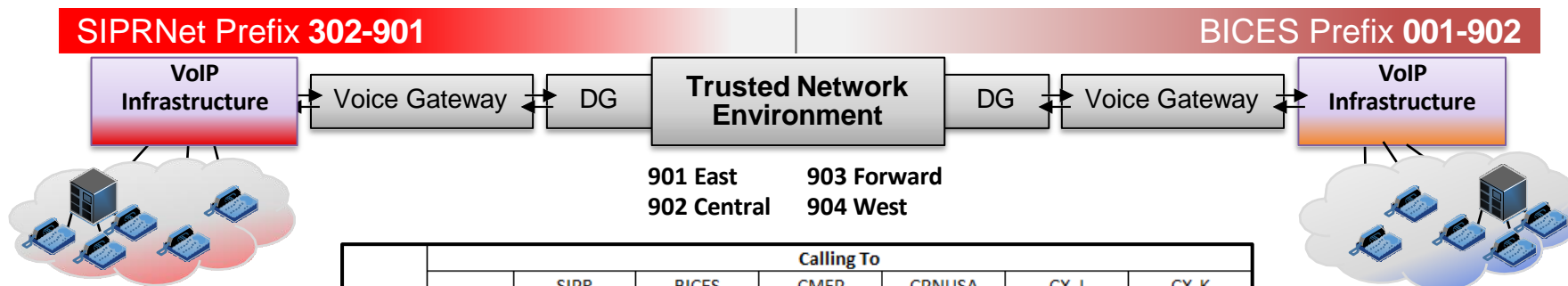
Making a Cross Domain Call



- User dials the appropriate cross-domain access number for the destination network being called (VoIP gateway dial plan number, usually 10 digits)
- User is greeted with “ To begin a cross domain call, enter the number you want to call, followed by pound or hash”
 - Then, enter the destination number followed by the pound or hash tag symbol
- Connects the call if the remote extension is allowed, on hold music until the receiving party answers
 - Call is rejected if the remote extension is not allowed or not valid
- Request VoIP dial plan from BICES-X service desk, government POC, or TNE on-site support



Cross Domain Calls



Note: Preferred access number is in green.

		Calling To					
		SIPR	BICES	CMFP	CPNUSA	CX-J	CX-K
Calling From	SIPR		302-902-9900	302-902-9933	302-902-9921	302-902-9981	302-902-9982
			302-902-8900	302-902-8933	302-902-8921	302-902-8981	302-902-8982
			304-901-9900	304-901-9933	304-901-9921	304-901-9981	304-901-9982
			305-903-9900	305-903-9933	305-903-9921	305-903-9981	305-903-9982
	BICES	001-901-9801			001-902-9921	001-902-9981	001-902-9982
		001-902-9801					
		001-904-9801					
	CMFP	631-243-9801					
		631-243-9701				631-243-9981	631-243-9982
		631-243-9601					
		631-243-9501					
	CPNUSA	611-500-9801					
		611-500-9701	611-500-9900			611-500-9981	611-500-9982
		611-500-9601					
		611-500-9501					
	CX-J	631-275-9801					
		631-275-9701	631-275-9900	631-275-9933	631-275-9921		631-275-9982
		631-275-9601					
		631-275-9501					
	CX-K	631-285-9801					
		631-285-9701	631-285-9900	631-285-9933	631-285-9921	631-285-9981	
		631-285-9601					
		631-285-9501					



Chat

UNCLASSIFIED



- TransVerse chat client end of life
- Supported chat client will be Swift, but TransVerse can still be used if available on the network
- TransVerse and Swift are interoperable
- Success based on network connectivity, and chat client correctly configured





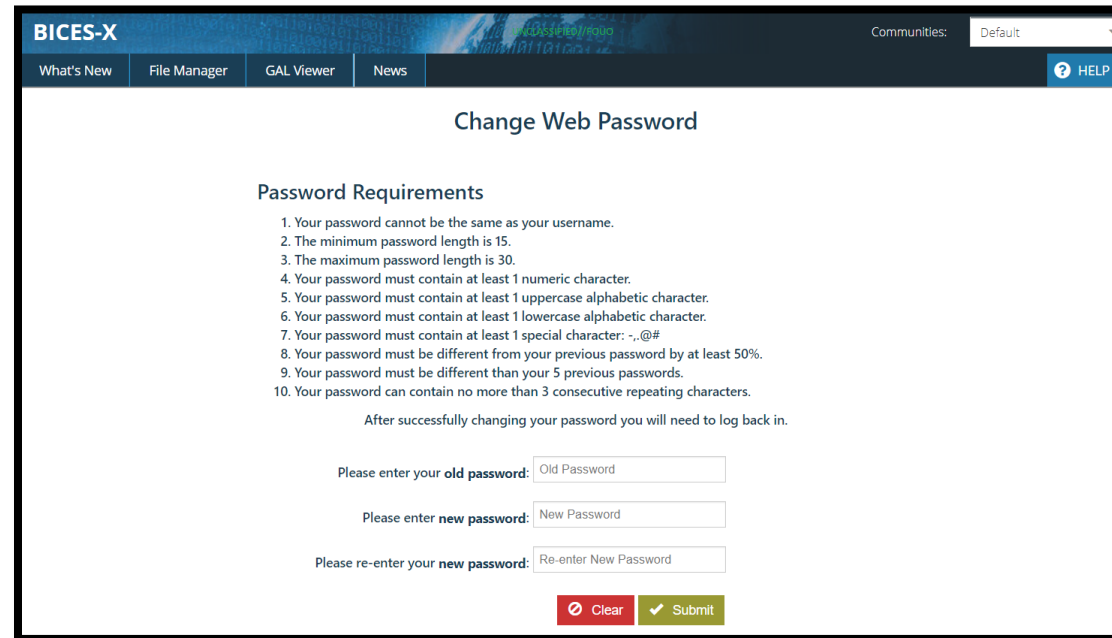
File Share

UNCLASSIFIED

- TNE users can access and share at the bilateral and multilateral level
- US Personnel can access the File Share from any interconnected network they have a system account on.
 - Same login (i.e. suserusa) used from any connection
 - Users cannot be logged into TNE Web from more than one network at a time (i.e., SIPR and BICES)
 - You will NOT see any data the connection you are connecting from is not cleared for
- To access:
 - 1. Access the ***File share service*** using the address provided when your account was created
 - 2. You will automatically be brought to the ***What's New*** page, which shows activity from the past 24 hours that users are allowed to see
 - Change password at your initial login
 - 3. Click the ***File Manager*** link in the menu header near the top of the page

Password Rules

- Passwords expire every 60 days
- After 60 days, website can't be accessed except to change password
- This grace period lasts for 21 days, after which time the account is locked
 - Account can be unlocked by calling the Help Desk
- New password complexity rules



The screenshot shows the BICES-X web interface. At the top, there's a navigation bar with 'What's New', 'File Manager', 'GAL Viewer', and 'News'. A 'Communities' dropdown menu is set to 'Default'. A 'HELP' button is in the top right. The main heading is 'Change Web Password'. Below it, 'Password Requirements' are listed as 10 numbered items. A note states: 'After successfully changing your password you will need to log back in.' There are three input fields: 'Please enter your old password:', 'Please enter new password:', and 'Please re-enter your new password:'. At the bottom are 'Clear' and 'Submit' buttons.

BICES-X Communities: Default

What's New File Manager GAL Viewer News ? HELP

Change Web Password

Password Requirements

1. Your password cannot be the same as your username.
2. The minimum password length is 15.
3. The maximum password length is 30.
4. Your password must contain at least 1 numeric character.
5. Your password must contain at least 1 uppercase alphabetic character.
6. Your password must contain at least 1 lowercase alphabetic character.
7. Your password must contain at least 1 special character: -.@#
8. Your password must be different from your previous password by at least 50%.
9. Your password must be different than your 5 previous passwords.
10. Your password can contain no more than 3 consecutive repeating characters.

After successfully changing your password you will need to log back in.

Please enter your **old password**:

Please enter **new password**:

Please re-enter your **new password**:

File Share Welcome Screen



- Landing page after login is the “What’s New” page

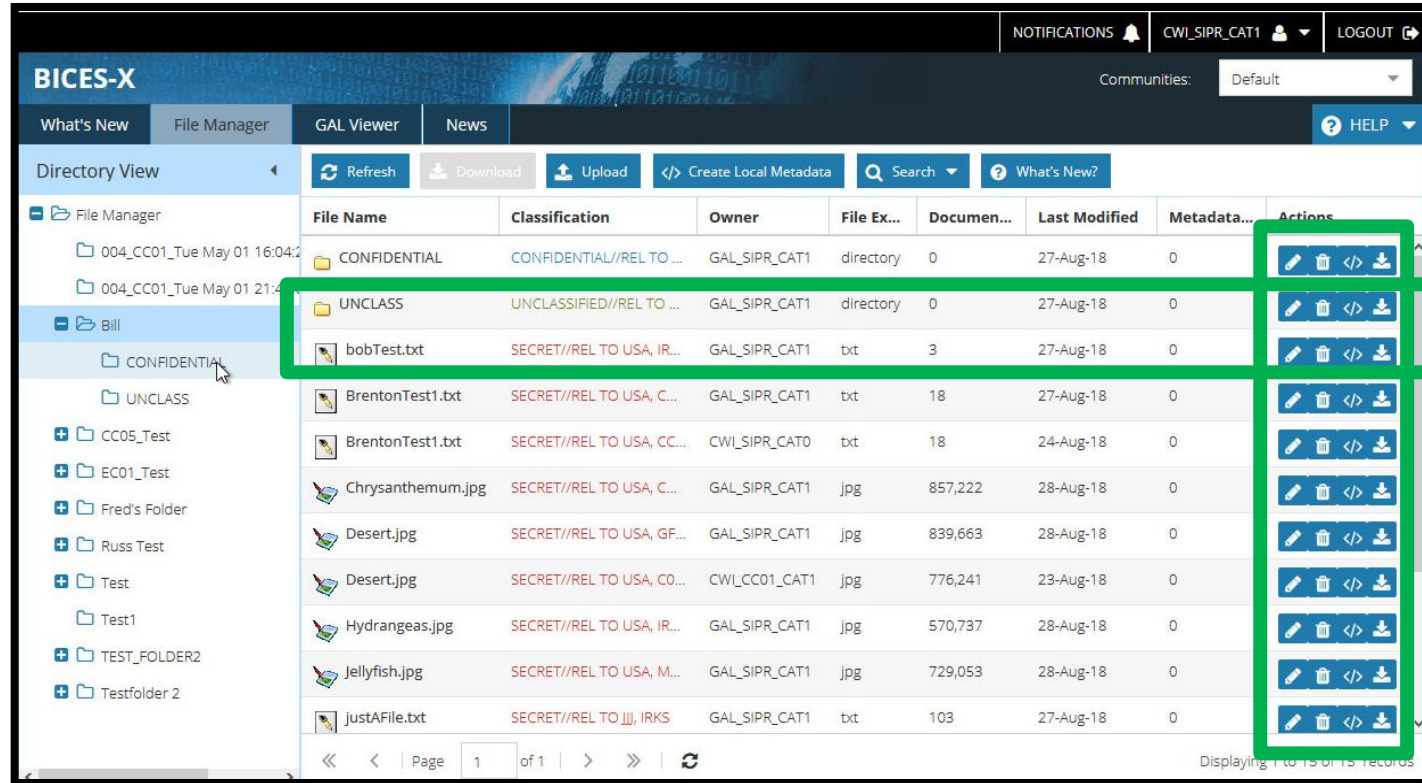
The screenshot displays the BICES-X File Manager interface. At the top, there is a header bar with the BICES-X logo, a 'Communities' dropdown menu, and navigation links for 'NOTIFICATIONS', 'GAL_CC01_CAT1', and 'LOGOUT'. Below the header, a secondary navigation bar contains tabs for 'What's New', 'File Manager', 'GAL Viewer', 'News', and 'CD View', along with a 'HELP' button. The main content area is titled 'Directory View' and features a table of files. The table has columns for 'File Name', 'Classification', 'Owner', 'File E...', 'Docume...', 'Last Modified', 'Metadat...', and 'Actions'. A single file is listed: '*NEW* five.txt' with classification 'SECRET//REL TO U...', owner 'GAL_CC01_...', and a size of 14 bytes. To the left of the table, there is a sidebar with a 'File Manager' icon and a 'CONFIDENTIAL' label. At the bottom, a pagination bar shows 'Page 1 of 1' and a status message 'Displaying 1 to 1 of 1 records'.

File Name	Classification	Owner	File E...	Docume...	Last Modified	Metadat...	Actions
NEW five.txt	SECRET//REL TO U...	GAL_CC01_...	txt	14	28-Feb-19	0	[Download Icon]



UNCLASSIFIED

- Folders are now displayed in the contents pane (on the right)



The screenshot displays the BICES-X File Manager interface. The left sidebar shows a directory tree with folders like '004_CC01_Tue May 01 16:04:2', '004_CC01_Tue May 01 21:4', 'CONFIDENTIAL', 'UNCLASS', 'CC05_Test', 'EC01_Test', 'Fred's Folder', 'Russ Test', 'Test', 'Test1', 'TEST_FOLDER2', and 'Testfolder 2'. The main pane shows a table of files and folders. A green box highlights the 'UNCLASS' folder and the 'bobTest.txt' file, indicating that folders are now displayed in the contents pane.

File Name	Classification	Owner	File Ex...	Documen...	Last Modified	Metadata...	Actions
CONFIDENTIAL	CONFIDENTIAL//REL TO ...	GAL_SIPR_CAT1	directory	0	27-Aug-18	0	[Icons]
UNCLASS	UNCLASSIFIED//REL TO ...	GAL_SIPR_CAT1	directory	0	27-Aug-18	0	[Icons]
bobTest.txt	SECRET//REL TO USA, IR...	GAL_SIPR_CAT1	txt	3	27-Aug-18	0	[Icons]
BrentonTest1.txt	SECRET//REL TO USA, C...	GAL_SIPR_CAT1	txt	18	27-Aug-18	0	[Icons]
BrentonTest1.txt	SECRET//REL TO USA, CC...	CWL_SIPR_CAT0	txt	18	24-Aug-18	0	[Icons]
Chrysanthemum.jpg	SECRET//REL TO USA, C...	GAL_SIPR_CAT1	jpg	857,222	28-Aug-18	0	[Icons]
Desert.jpg	SECRET//REL TO USA, GF...	GAL_SIPR_CAT1	jpg	839,663	28-Aug-18	0	[Icons]
Desert.jpg	SECRET//REL TO USA, CO...	CWL_CC01_CAT1	jpg	776,241	23-Aug-18	0	[Icons]
Hydrangeas.jpg	SECRET//REL TO USA, IR...	GAL_SIPR_CAT1	jpg	570,737	28-Aug-18	0	[Icons]
Jellyfish.jpg	SECRET//REL TO USA, M...	GAL_SIPR_CAT1	jpg	729,053	28-Aug-18	0	[Icons]
JustAFile.txt	SECRET//REL TO III, IRKS	GAL_SIPR_CAT1	txt	103	27-Aug-18	0	[Icons]

- Pre-defined folder structure
- Users will only see folders and files:
 - That are marked REL to the network they are accessing
 - From the restrictions on their TNE log-in account
- Folder icons have meaning

Public Folder Icon	Private Folder Icon	Public Folder with Metatdata	Private Folder with Metatdata
			

- Stringent restrictions upon characters allowed by the Web
 - Dash (-) no longer permitted in file name
- File names permit this:
 - Alphabet, numeric, the at symbol '@', plus, period
 - Spaces are automatically converted to underscores
- Other text fields (such as folder names, Saved search names, and GAL fields permit):
 - Alphabet, numeric, space, - (dash), comma, period and @ characters only

- Users will be granted permission to operate within three user categories, or levels of access:
 - **Category 3** (Download files in shared folders) – Majority of Category 3 users must identify any inappropriately marked products to a Category 1 user if they own the product
 - **Category 2** (Download and Upload files to shared folders) – Users will be allowed to:
 - Manage content on assigned folders
 - Upload documents on behalf of Category 3 users, as required
 - **Category 1** (Download, Upload, and Relabel) – Users will be allowed to change classification and releasable information in the shared folders
 - Only authorized to relabel files they own and cannot relabel files uploaded by other users (**Default Users – Majority of I-P Users will be in this category**).

File Share Levels of Access



File Permissions								
	Read	Download	Upload	Write	Move	Copy	Delete	Re-Label
Category 1 (CAT1)	x	x	x	x	x	x	x	x
Category 2 (CAT2)	x	x	x	x	x	x	x	
Category 3 (CAT3)	x	x						

Folder Permissions						
	Edit Properties	Create	Move	Copy	Delete	Re-Label
Category 1 (CAT1)	x	Permissions allowed on owned or managed folders only.				
		x	x	x	x	x
Category 2 (CAT2)						
Category 3 (CAT3)						

Users are responsible for ensuring security classification markings are placed correctly on finished products prior to posting. Report any “spillages” to your COCOM J6 help desk and the Coalition Support Service Desk.



Create & Manage New Directory



- Creating subfolders
 - R-click on a main folder
 - Select “Create New Directory”
 - Users need to follow local command’s
 - directory creation policies.
 - Only TNE Admin can create a new folder at the root level, and additional approvals from Ops Manager (CTR) and/or Operations Chief (GOV) are needed
- Folder owners can:
 - Change Label/Classification
 - You can accidentally "hide" data. Ex: changing the label on a folder that was NATO and contains NATO data to FVEY. BICES would no longer be able to see this folder full of NATO data.
 - Delete
 - Make Private
 - Manage Folder



UNCLASSIFIED

File Upload: Multi-File Uploader



- File upload via a single window (not three separate windows)
 - Select **Upload** → Select **Browse...** navigate to your product → R-Click on product to select classification → Select **Upload** → **Auto Updates** are on by default → When Status is **Review and accept changes** select file and click **Accept Checked Submissions**

BICES-X

What's New | File

Directory View

File Manager

Pre-processing Queue

Finalization Queue

Upload File: Bill

11S Multi-file Uploader

Browse... Upload Abort Metadata Uploader Remove selected Remove all

Filename	Security Label?	Size	File Ext...	Sta...	%
1 cc08_sipr.txt	Right click here to set security label			default	0%

Selected 1 file(s), 4 bytes

File Upload Statuses

Refresh Queue Accept Checked Submissions Deny Checked Submission

File Name	Security Label	File Ext...	Date	File Path	Status	Changes	Meta...
-----------	----------------	-------------	------	-----------	--------	---------	---------

Auto Updates: updates the status window every 10 seconds



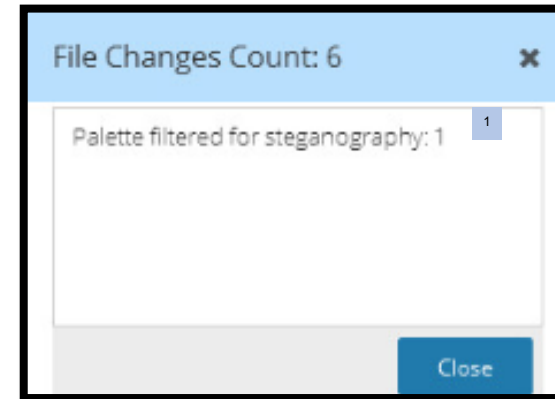
UNCLASSIFIED

File Upload: Multi-File Uploader

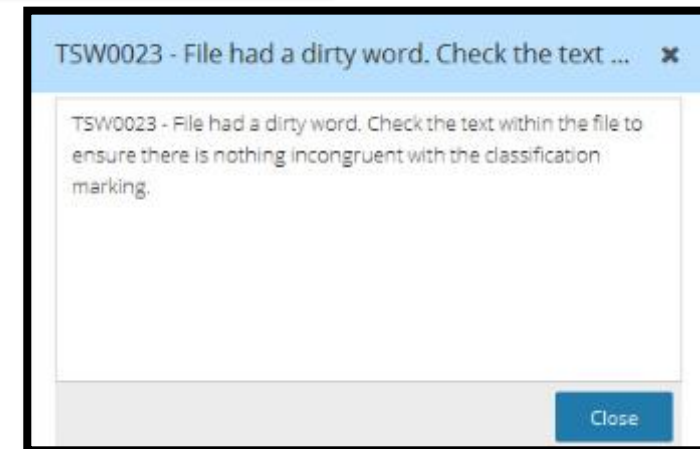


File Upload Statuses						
<div><div>Refresh Queue</div><div>Accept Checked Submissions</div><div>Deny Checked Submissions</div></div>						
<input type="checkbox"/>	File Name	Security Label	File Extension	Date	File Path	
<input type="checkbox"/>	secondary01UploadFil...	SECRET//REL TO USA, C01	txt	2019-04-22	/Testfolder 2/Laura's Test/	
						<div><div>Status</div><div>Changes</div><div>Metadata</div></div>
						<div><div>Review</div><div>View Su...</div><div>N</div></div>

- Summary of filtered file changes



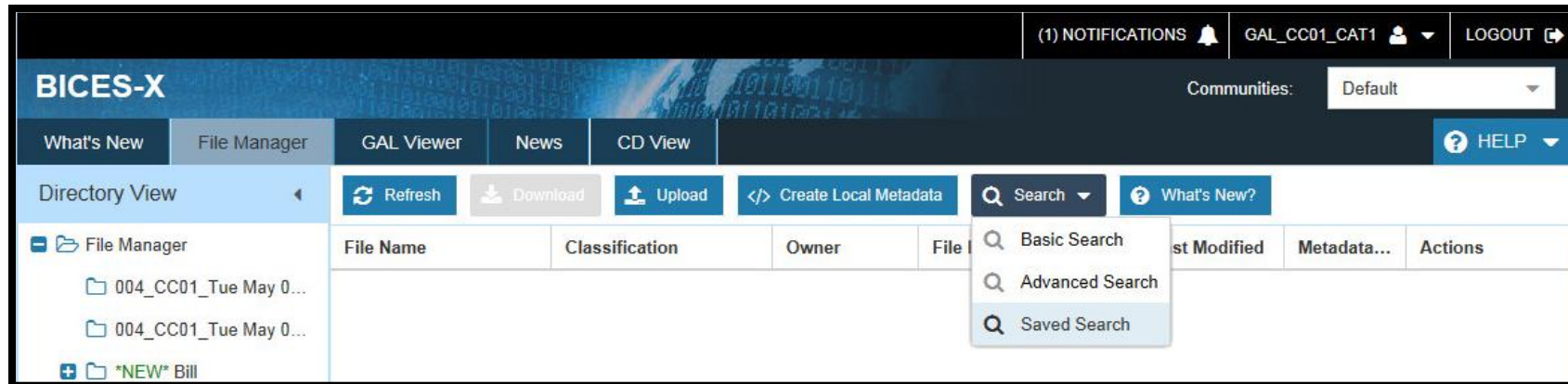
- Improved error messages on rejected files



- A single file can be downloaded by:
 1. action icon
 2. double-click on the file
 3. right-click context menu on the file
 4. download button on toolbar
- Multiple files can be downloaded
 - Select multiple files using either Shift-Click or Control-Click
 - All files must be in the same folder
 - All selected files downloaded into a single .zip file
 - Maximum size of file selection: 250 MB
 - Maximum number of files: 25

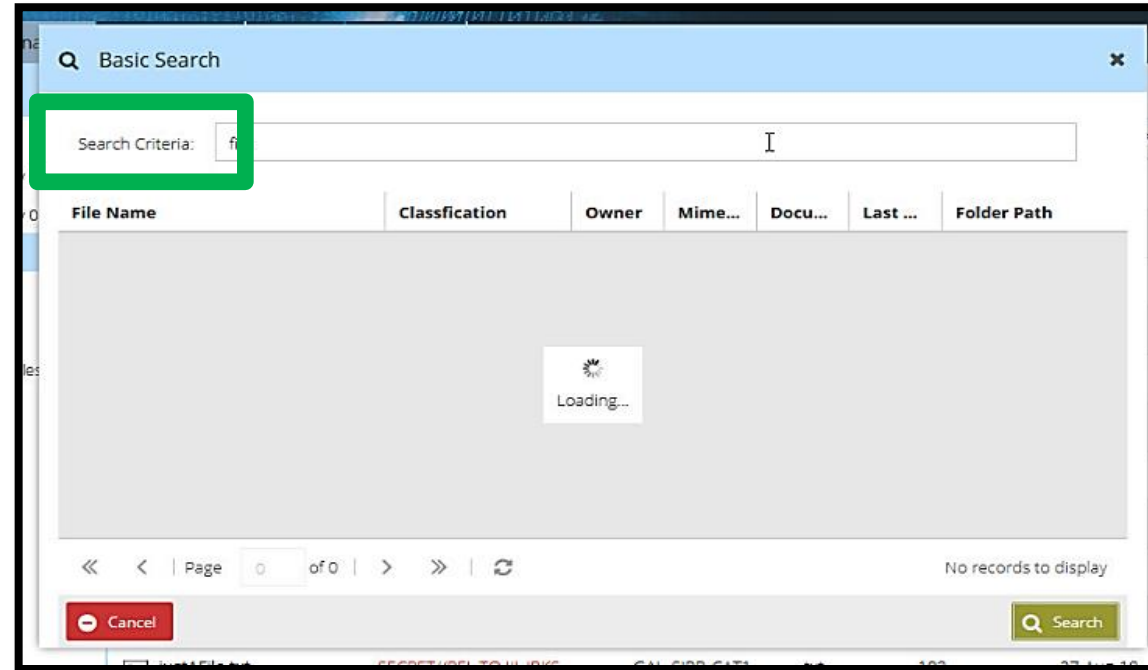
- Authorized file types:
 - **Word Processing:** .doc .docm .docx
 - **Spreadsheets:** .xls .xlsm .xlsx
 - **PowerPoint:** .pps .ppsm .ppsx .ppt .pptm .pptx
 - **Archives:** .bz .bz2 .gz .tar .zip
 - **Text-based:** .csv .log .txt .xml
 - **Graphics:** .apm .bmp .dib .dws .emf .gif .j2c .j2k .jfi .jfif .jif .jp2 .jpc .jpe .jpeg .jpf .jpg .jpg2 .jpx .png .tif .tiff .wmf
 - **Portable Documents:** .pdf
- 250 MB file size limit
- Multi-file uploader allows selection of 25 files at a time for upload
- Refresher (no changes)
 - No encrypted files
 - Dirty word filter still in place
 - HTML is unsupported

1. Basic Search – a single search field “like Google”
2. Advanced Search – search on many different criteria
3. Saved Search – save your searches and run them again later



Basic Search

- Enter a text string: searches file name, folder name, file contents



- Slowest search, but easiest to operate
- Tired of waiting? Use Advanced Search



Advanced Search



- Search by criteria:
 - File/Folder Name
 - File Contents
 - Owner
 - Limit within Folder & sub-folders
 - Date Search
 - Mime Type
 - Classification

Search Options:

Multi-Field Logic: **And, Or**

- When multiple criteria are used, this sets the logical operator to tie them together.
For example: **Owner AND/OR Classification**

The screenshot shows the 'Advanced Search' window. On the left, a sidebar has 'File' and 'Metadata' tabs. The 'File' tab is active, showing search criteria: 'Entry 1: Contains file', 'Operator: AND', and 'Limit by Folder' (checked). Below these are expandable sections for 'Content', 'Owner, Folder Name', 'Options', 'Date Selection', 'Mime Type', and 'Classification'. The results table below shows four entries, all named 'justAFile.txt', with various classifications and owners. The bottom of the window includes a 'Cancel' button, a 'Save Search' button, and a 'Search' button.

File Name	Classification	Owner	Mime T...	Docum...	Last M...	Folder Path
justAFile.txt	SECRET//REL TO USA, ...	GAL_SIP...	text/plain	103	27-AUG...	/Bill/
justAFile.txt	SECRET//REL TO USA, ...	GAL_SIP...	text/plain	103	27-AUG...	/Bill/
justAFile.txt	SECRET//REL TO USA, ...	CWL_SIP...	text/plain	103	22-AUG...	/Bill/
justAFile.txt	SECRET//REL TO JJJ, IRKS	GAL_SIP...	text/plain	103	27-AUG...	/Bill/

- Search: Files Only, Metadata Only, Folders, or Files & Folders
- File Name Exact Match
- Note that if folders-only is selected, some search criteria will be ignored if it doesn't pertain to folders, for example "file name"



UNCLASSIFIED

Search: Keep in Mind

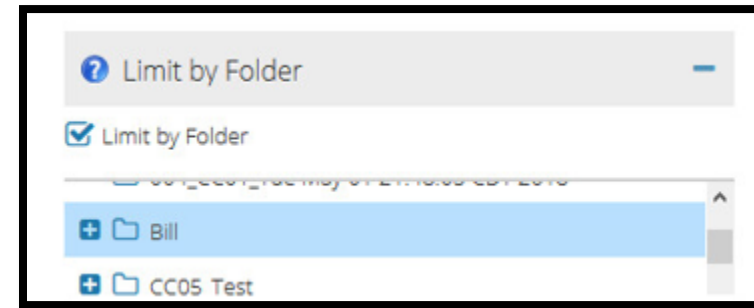


- The following MIME types **cannot** be searched for content (other search criteria like file name, date, and etc is supported)
 - -application/zip
 - -image/jpeg
 - -application/octet-stream
 - -application/x-tar
 - -image/gif
 - -application/x-compressed
 - -application/x-gzip
 - -image/png
 - -image/bmp
 - -Microsoft Office 2013 (and beyond).
- Search fields permit this:
 - Alphanumeric, dot, parenthesis, space, underscore



UNCLASSIFIED

- Search Options supporting multi-select
 - Limit by Folder
 - Mime Type
 - Classification



- ❖ Tip: File Content Search is the slowest type of search ; avoid it unless you need it
 - (this is why Basic Search is slow)

Search Results



- Sort the search results by clicking on column header

File Name	Classification	Owner	Mime T...	Docum...	Last M...	Folder Path
 justAFile.txt	SECRET//REL TO USA, ...	GAL_SIP...	text/plain	103	27-AUG-...	/Bill/
 justAFile.txt	SECRET//REL TO USA, ...	GAL_SIP...	text/plain	103	27-AUG-...	/Bill/
 justAFile.txt	SECRET//REL TO USA, ...	CWL_SIP...	text/plain	103	22-AUG-...	/Bill/

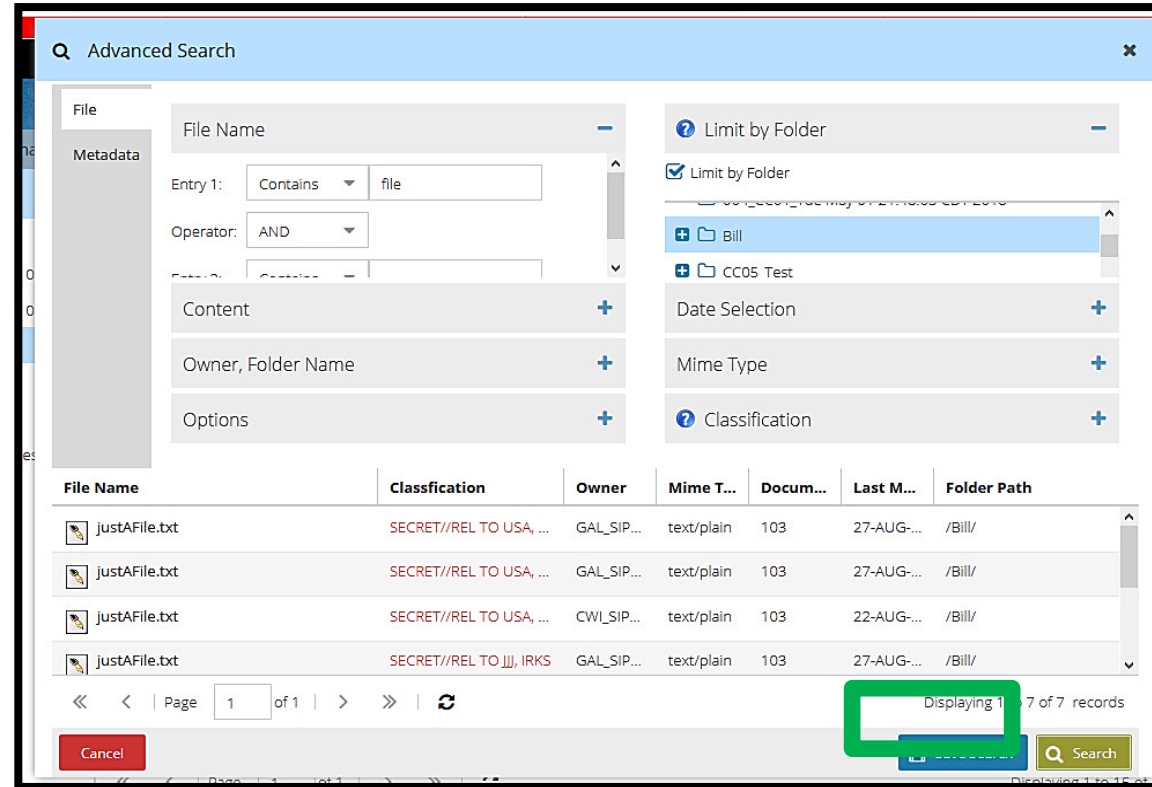
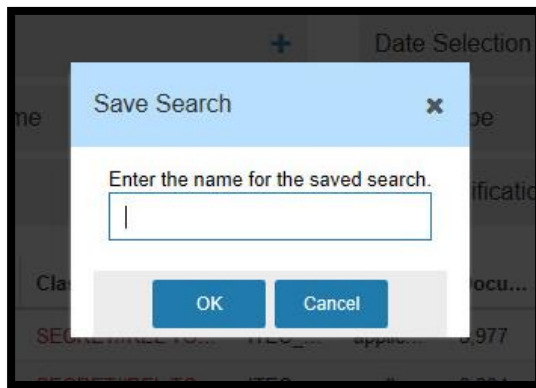
- Actions (right-click on a search result):
 - Locate Item
 - Takes File Manager to the folder and closes the Advanced Search Screen
 - Download selection (one to many)
 - Download the selected files. Use Shift-Click or Control-Click to select multiple.
 - Download All...
 - Clear filtering
 - Clears the column header filters (if you clicked on the column headers)
 - Clear Panel
 - Clears the search results
- ❖ Tip: the Advanced Search screen retains all user input when closed and re-opened (so that you don't lose the search parameters you've entered). To clear all parameters, use the Reload button on the web browser.



Saved Search



- Advanced Searches can be Saved on the Advanced Search screen and then retrieved on the Saved Search screen under the Search dropdown menu



UNCLASSIFIED

Saved Search



Available Fields

Select a field to add it to the query

fileName
classification
content

Selected Field

Value

fileName{"value1": "file", "qualifie...

Saved User Queries

FileSearch2

SearchforFile

Built Query:

```
{
  "file": {
    "fileName": {
      "value1": "file",
      "qualifier1": "Contains"
    }
  },
  "preferences": {
    "searchPreference": "FILE",
    "multipleFieldsOperator": "AND",
    "searchAllPreference": "Files Only",
  }
}
```

File Name	Classification	Ow...	Mi...	Do...	La...	Folder Path
BH_Test_file8.docx	SECRET//RE...	ITE...	app...	8,977	02-...	/Testfolder 2/
BH_Testfile_10.docx	SECRET//RE...	ITE...	app...	8,984	21-...	/TEST_FOLD...
BH_Testfile_12.docx	SECRET//RE...	ITE...	app...	8,984	02-...	/Testfolder 2/
fed003_pubFile.tct_-_C...	SECRET//RE...	FE...	text...	24	31-...	/Testfolder 2/...

<<

<

Page 1 of 1

>

>>

Displaying 1 to 13 of 13 records

Close



Saved Search



- 1- list of saved searches 2 – available search criteria 3- search criteria data 4 – selected field
5 – search results 6 – add new saved search 7 – delete selected saved search 8 – the full query

6

7

1

8

2

3

4

5

Available Fields

fileName

classification

content

Select a field to add it to the query

3

Selected Field

Value

fileName

{"value1": "file", "qualifie..."}

4

Built Query:

```
{
  "file": {
    "fileName": {
      "value1": "file",
      "qualifier1": "Contains"
    }
  },
  "preferences": {
    "searchPreference": "FILE",
    "multipleFieldsOperator": "AND",
    "searchAllPreference": "Files Only",
  }
}
```

8

File Name	Classification	Ow...	Mi...	Do...	La...	Folder Path
BH_Test_file8.docx	SECRET//RE...	ITE...	app...	8,977	02-...	/Testfolder 2/
BH_Testfile_10.docx	SECRET//RE...	ITE...	app...	8,984	21-...	/TEST_FOLD...
BH_Testfile_12.docx	SECRET//RE...	ITE...	app...	8,984	02-...	/Testfolder 2/
fed003_pubFile.tct_- _C...	SECRET//RE...	FE...	text...	24	31-...	/Testfolder 2/...

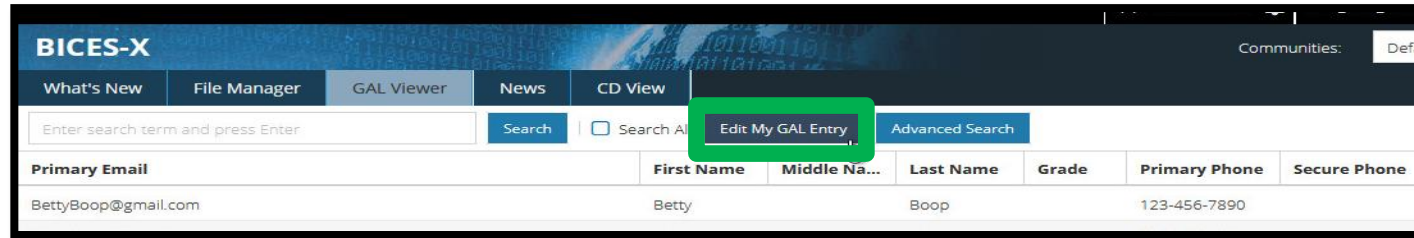
Page 1 of 1

Displaying 1 to 13 of 13 records



- Saved searches are not shared. Only you can see your saved searches.
 - Saved Search screen allows:
 - Viewing of saved searches
 - Execution of saved searches
 - Construction of saved searches
 - Modification of saved searches
 - Deletion of saved searches
 - Each user can have a maximum of 25 saved searches
- ❖ Tip: Multiple saved searches can have the same name (this is confusing and not recommended— you'll want to enter unique names)

- You can now edit parts of your GAL entry



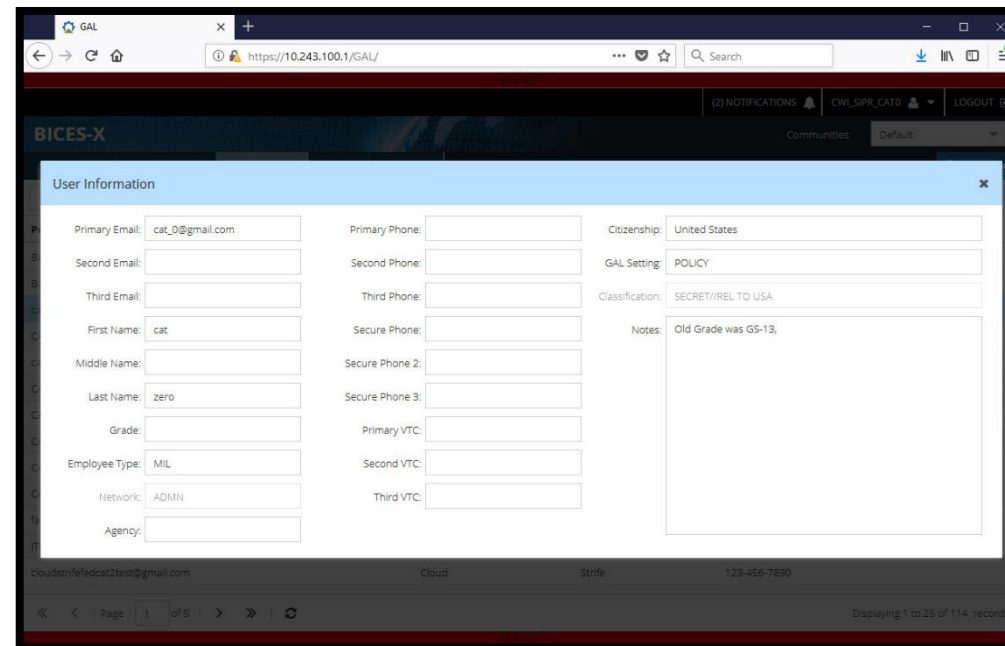
BICES-X Communities: Default

What's New | File Manager | **GAL Viewer** | News | CD View

Enter search term and press Enter ☐ Search All **Edit My GAL Entry**

Primary Email	First Name	Middle Na...	Last Name	Grade	Primary Phone	Secure Phone
BettyBoop@gmail.com	Betty		Boop		123-456-7890	

- Updateable fields: 2nd & 3rd Email, Grade, Employee Type, Agency, Phone (all), Secure Phone (all), VTC (all), Agency



BICES-X Communities: Default

(2) NOTIFICATIONS CWI_SPR_CATO LOGOUT

User Information

Primary Email: cat_0@gmail.com Primary Phone: Citizenship: United States

Second Email: Second Phone: GAL Setting: POLICY

Third Email: Third Phone: Classification: SECRET//REL TO USA

First Name: cat Secure Phone: Notes: Old Grade was GS-13,

Middle Name: Secure Phone 2:

Last Name: zero Secure Phone 3:

Grade: Primary VTC:

Employee Type: MIL Second VTC:

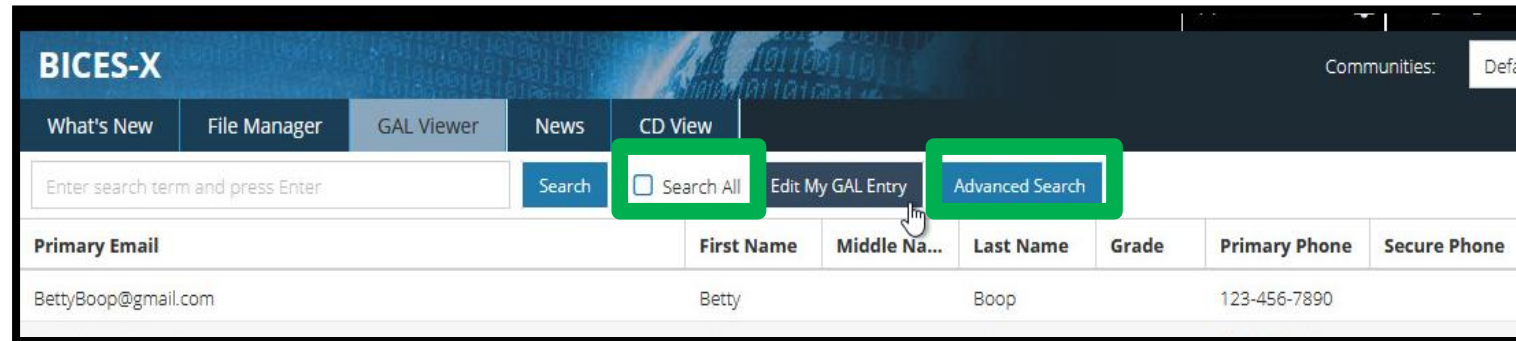
Network: ADMIN Third VTC:

Agency:

cloudstrifeedcat2test@gmail.com Cloud Strife 123-456-7890

Page 1 of 5 Displaying 1 to 25 of 114 records

- Search is expanded



The screenshot shows the BICES-X web application interface. At the top, there's a navigation bar with tabs: What's New, File Manager, GAL Viewer, News, and CD View. Below this is a search section with a text input field labeled "Enter search term and press Enter", a "Search" button, a "Search All" checkbox (highlighted with a green box), an "Edit My GAL Entry" link, and an "Advanced Search" button (also highlighted with a green box). Below the search section is a user profile table with the following data:

Primary Email	First Name	Middle Na...	Last Name	Grade	Primary Phone	Secure Phone
BettyBoop@gmail.com	Betty		Boop		123-456-7890	

- Search common fields in the text box
 - Same as in Release 3.0
- Search all GAL fields with the “Search All” checkbox
- Advanced Search: search on specific fields
 - Network, Employee, Citizenship, Agency
 - Each has a dropdown of allowed values
 - Advanced Search will only search these selected fields (ignores anything in the text box)

- Three fields are now a drop-down list of enumerated values provided by the BICES Program Office
 - - Citizenship field
 - An enumerated list of government agencies
 - - Employee Type
 - An enumerated list: CIV, CTR, or MIL
 - - Grade
 - An enumerated list: E-1 through E-9, W-1 through W-5, O-1 through O-11, GS-1 through GS-15, SES-1 through SES-15, and Blank is allowed (for people who don't have grades, like contractors).
 - Users can add enter their own Grade text too



Email & File Share Rejection Fixes

UNCLASSIFIED

Email & File Share Rejection Fixes



- Ensure your document has a REL TO caveat in the classification marking
 - UNCLASSIFIED alone is not authorized... must contain a REL caveat
- Remove unnecessary Slide Master Formats and check markings
- If all else fails, save your product as a PDF
- Users will receive improved error rejection messages which will provide details as to why a transfer was not successful.



UNCLASSIFIED

Email & File Share Rejection Fixes



- White-on-white / black-on-black camouflaged text (Word, Powerpoint, Excel)
- (Excel) columns/rows too narrow
- Overlapping/obscured images (PowerPoint especially)
- Headers and footers are allowed, but often have dirty words or hidden text in them (PowerPoint especially)
- Has Hyperlinks (Word, PowerPoint, Excel)
- Excessive image resizing –Image cropping does not remove the part of the image that can no longer be seen– cropping only changes the viewport of the image– the image is still there!
- Column data hiding in extreme locations
- (PowerPoint) Don't forget to check the Master Slide(s) for issues
- Remove metadata (File->Info->Check for Issues->Inspect->Remove All)



Email & File Share Rejection Fixes



- Inspect the file for issues
 - Remove Header/Footer (not in word)
 - Embedded documents, Macros, forms, ActiveX controls, Custom XML Data, Invisible Content, **Off Slide Content**, Comments, **Overlapping boxes** and Notes just to name a few...
- Fix classification markings to comply with DoD classification requirements in accordance with SMP/DoDM 5200.01 v2
 - Note that UNCLASSIFIED must still contain a releasability caveat
- Ensure classification markings are correct
 - COMMON MISTAKE: A period vs. a comma is used or putting an extra space
 - Correct: SECRET//REL TO USA, MESF
 - Incorrect: SECRET//_REL TO USA. MESF
- Examples of Dirty Words: CONFIDENTIAL, SECRET, S//, (C//, CUI, (CUI//
 - Do a keyword search for those terms



UNCLASSIFIED

Email & File Share Rejection Fixes



- To check a file for issues that may cause rejection:

1. Click **File**
2. Click **Info**
3. Click **Check for Issues**
4. Click **Inspect Document**
5. Check items to inspect
6. Click **Inspect**
7. Remove issues
8. Re-inspect
9. Save the file

1.

2.

3.

4.

5.

6.

7.

8.



UNCLASSIFIED

- Metadata is data about data
 - In TNE12S Web, Metadata is stored in files
 - Metadata files are .XML files (DDMS v5.0)
 - Metadata files are also filtered
 - And therefore, can pass or fail during upload
 - Metadata files must be associated with a regular file, or a folder
- ❖ The contents of the metadata file should describe the file or folder that it is associated with (it's data about data!)



- DDMS v5.0 is the metadata standard supported in this release
- DDMS v5.0 has fields like:
 - Security markings
 - Document Creator
 - Document Publisher
 - Date
 - Document Point of Contact
 - Country of Origin
 - Document Subject
 - Category, Keyword, Actor, etc
 - And many more!



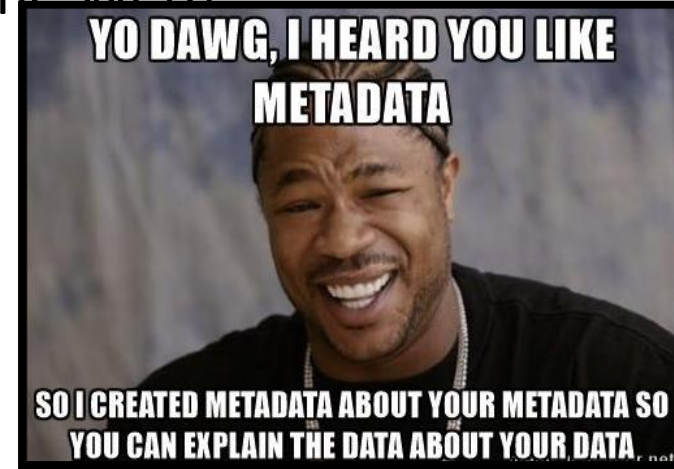
❖ These fields are used to describe the file or folder that the metadata file is associated with

- What are all the things I can do with metadata on the Web?

1. Upload it
2. Download it
3. Delete it
4. Create it
5. Edit it

- The real reasons for doing all of the above:

6. Search for it



6. Search for the metadata to find files/folders with it

- ❖ Example: find all files with Publisher “34th Intelligence Squadron”
- ❖ Example: find all folders with Subject keyword “BoldQuest 2018”

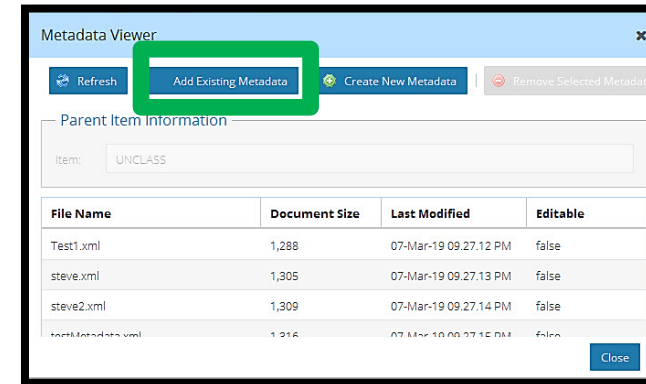
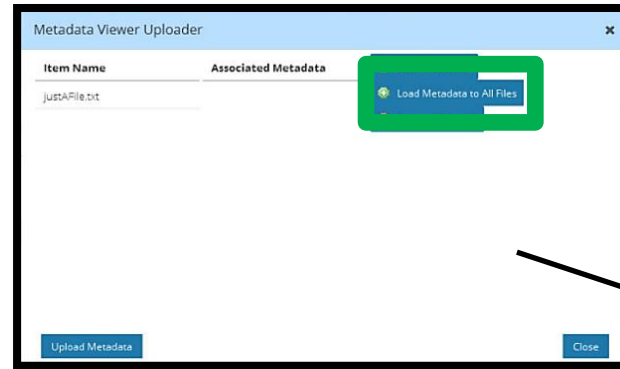
- What else?
8. If you move a file or folder with metadata, the metadata moves too (automatically)
 9. If you delete a file or folder that has metadata, the metadata is deleted too (automatically)
 10. If you re-label a file or folder with metadata, the metadata is re-labeled too (automatically)
 - Note: the metadata file always has the same security marking as the file/folder it is associated with



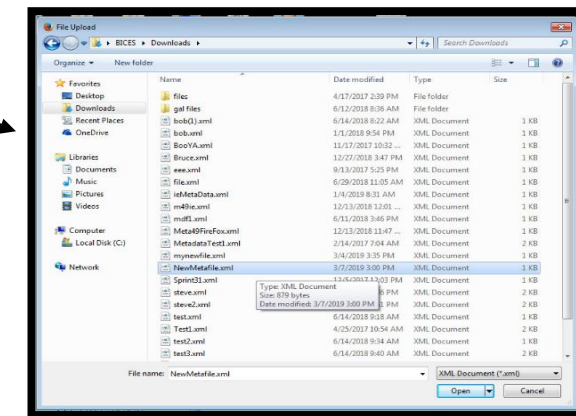
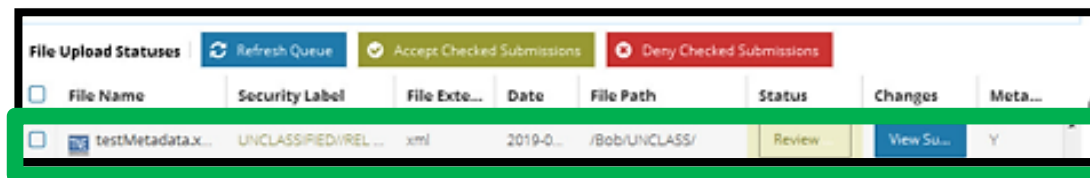
- Because metadata is new to TNE 4.0, is no existing metadata in the system
 - Not even for existing files & folders!
- Metadata comes from you! The users.
- It is optional → a new file or folder can be created without metadata
- Metadata can be added to any file or folder, provided you have the necessary permissions to see the file or folder, and the ability to upload files to the WEB
 - CAT 3 user cannot upload

1. Upload Metadata

- Method 1: Upload a .XML metadata file and associate with an **existing** file or folder
- This is the method to use when you already have a .XML metadata file
 1. Right-click on target file or folder, click View Metadata
 2. Click Add Existing Metadata
 3. Click Load Metadata, then use File Browser

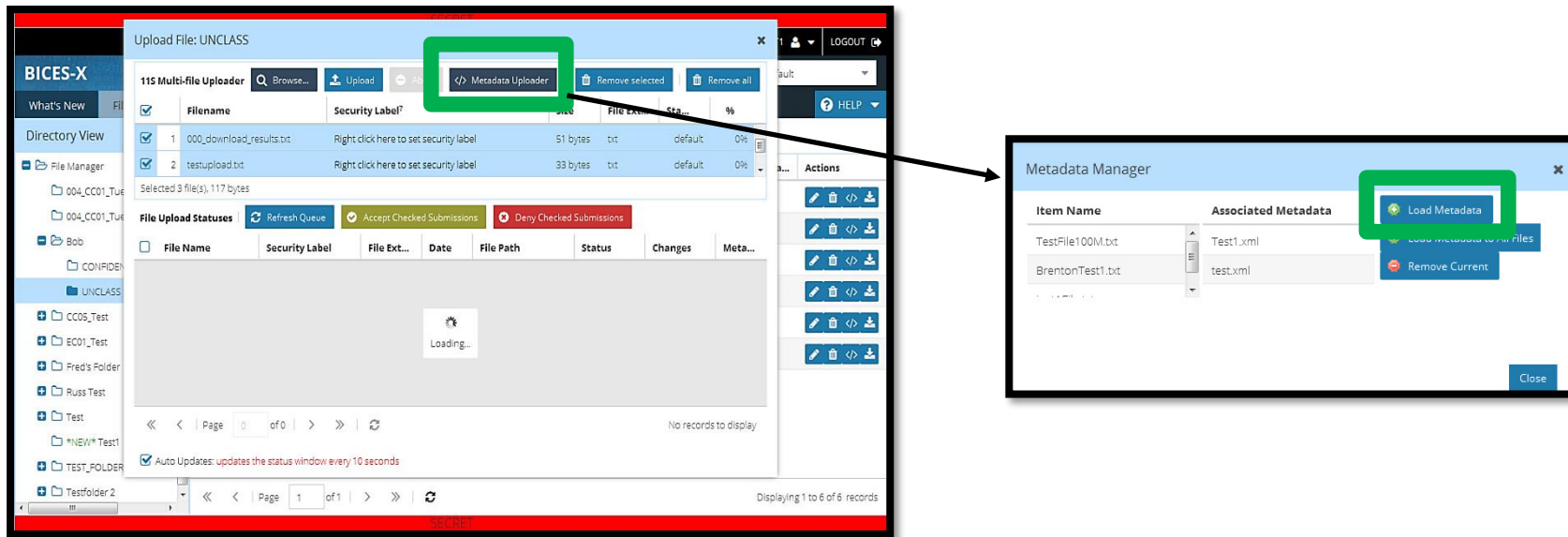


4. Click Upload
5. Navigate to the File Manager Upload screen to view and accept the filtered metadata file



1. Upload Metadata

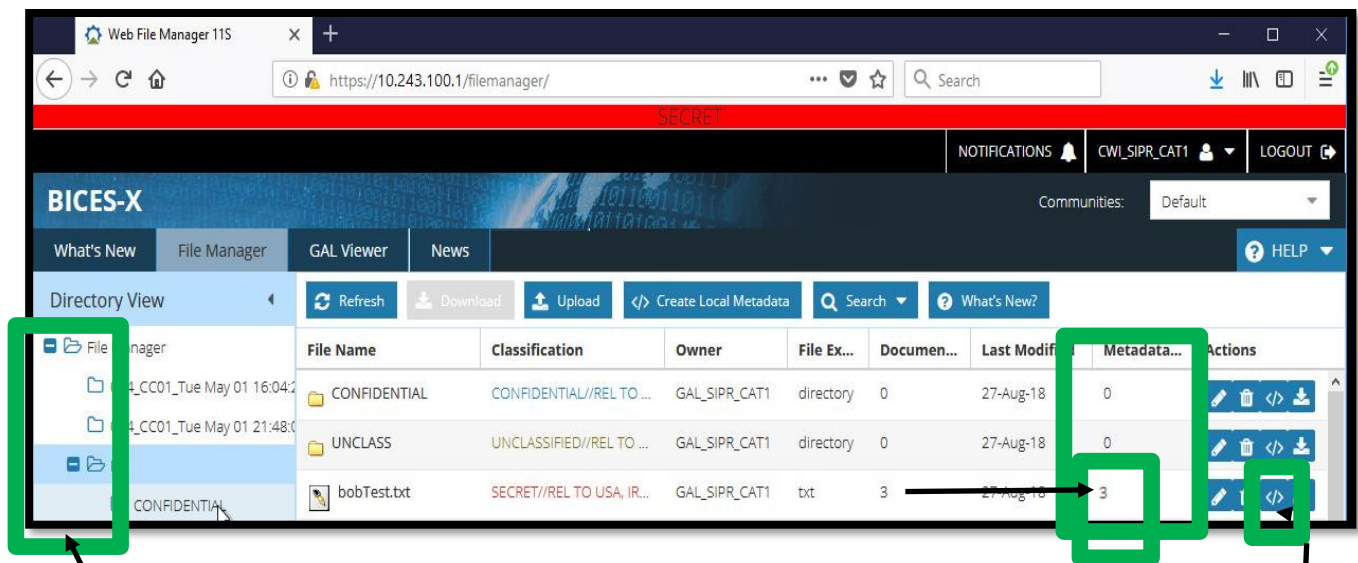
- Method 2: Upload a .XML metadata file along with a **new** file being uploaded
 - Begin a file upload as normal
 - Add Metadata to the file
 - Set the Security Label (same for file & metadata), then Upload
 - View upload progress as normal (bottom portion of the upload screen)
 - It is possible for the file to pass the filter, but the metadata file could fail the filter



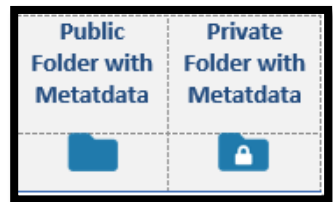
2. Download Metadata



- How do you know if there is associated Metadata?
- Look at the File Manager

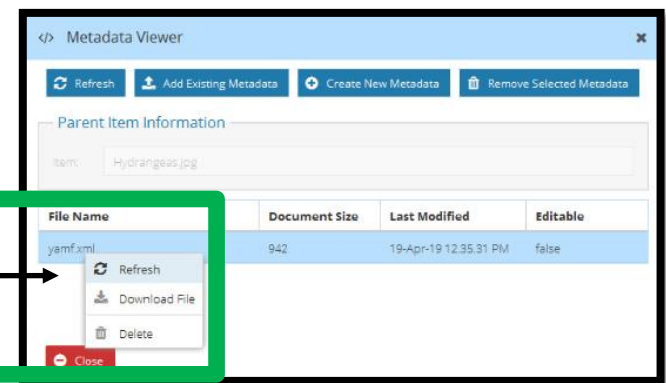


Folder icons show if associated metadata



three metadata files associated with the "bobTest.txt" file

Metadata action button



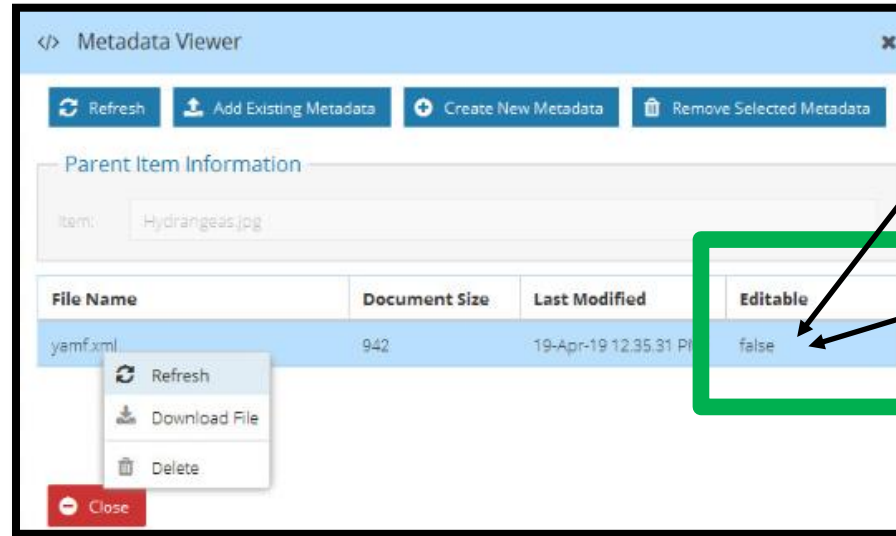
Right-click to download metadata



2. View Metadata

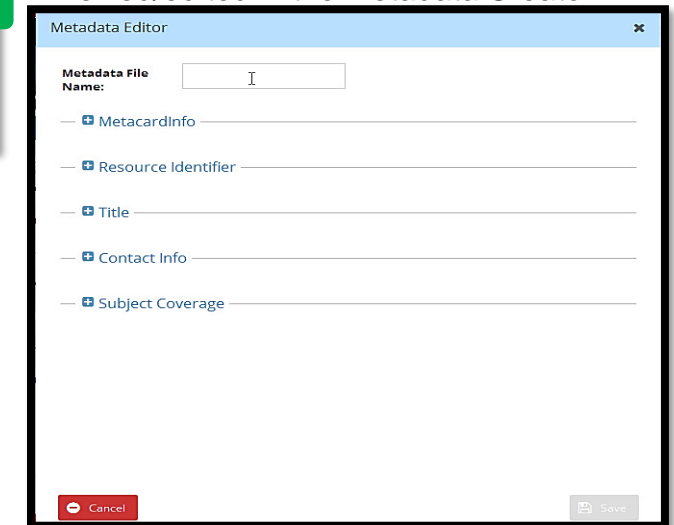


- Option 1: once the .XML file is downloaded to your computer, you can open it with an XML viewer or just a text viewer (XML is text)
- Option 2: Metadata Viewer screen



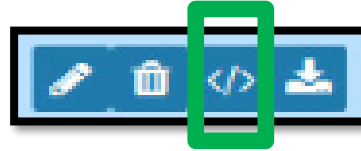
FALSE: Metadata was not created using the Web's Metadata Creator, and therefore cannot be opened in the Metadata Creator

TRUE: Metadata Creator used to create the metadata, and therefore it can be viewed/edited in the Metadata Creator

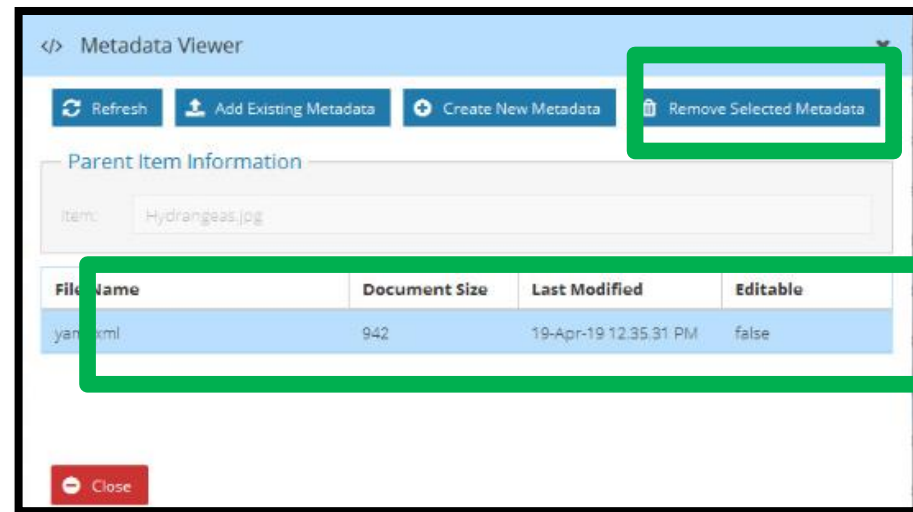


3. Delete Metadata

1. Use the Metadata Action Button
 - Or, Right-click on a folder for file containing Metadata, or Select **>View Metadata** from the menu



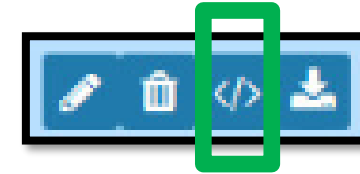
2. From the **Metadata Viewer** window select the Metadata file to be downloaded from the list shown
3. Click **>Remove Selected Metadata** button from the toolbar at the top of the Metadata Viewer window



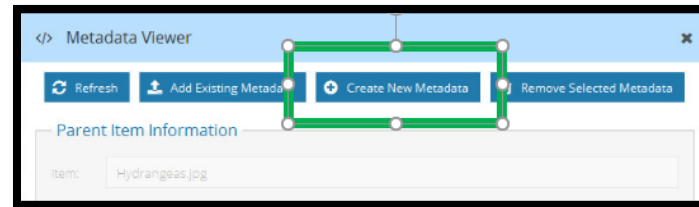
4. Create Metadata



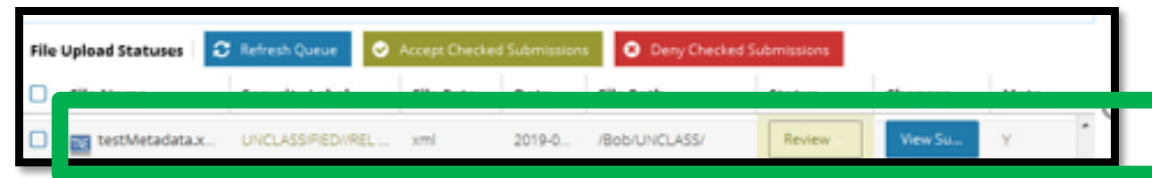
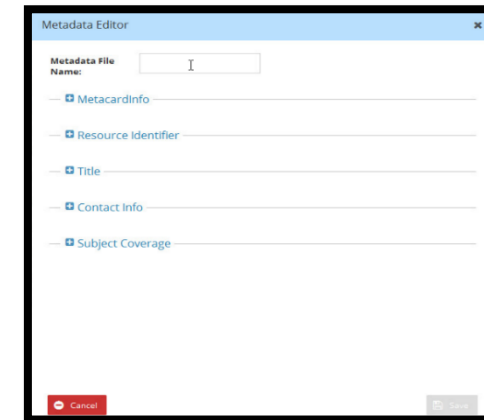
1. Use the Metadata Action Button on a file
 - Or, Right-click on a folder for file containing Metadata, or Select **>View Metadata** from the menu



2. From the **Metadata Viewer** window click **Create New Metadata**



3. Enter a metadata filename, and enter the metadata fields
4. When done, press Upload
5. Navigate to the File Manager Upload screen to view and accept the filtered metadata file

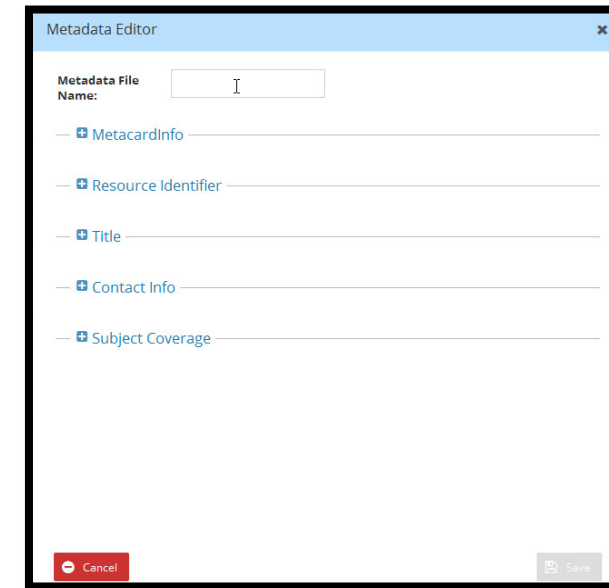
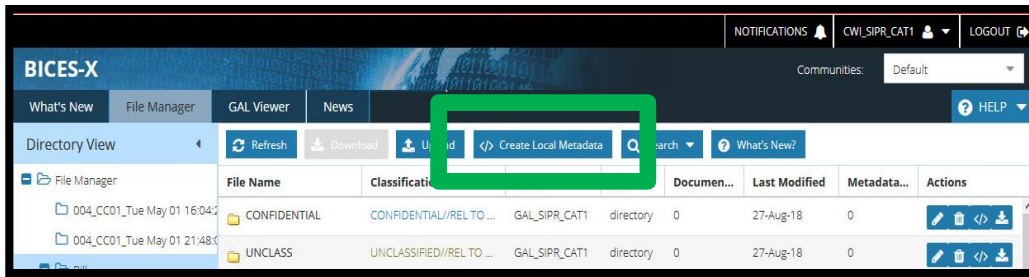


UNCLASSIFIED

4. Create Metadata

- You can also use the Web to create a .XML metadata file and save it directly to your computer (it never goes into the Web)

1. In File Manager, click **Create Local Metadata**

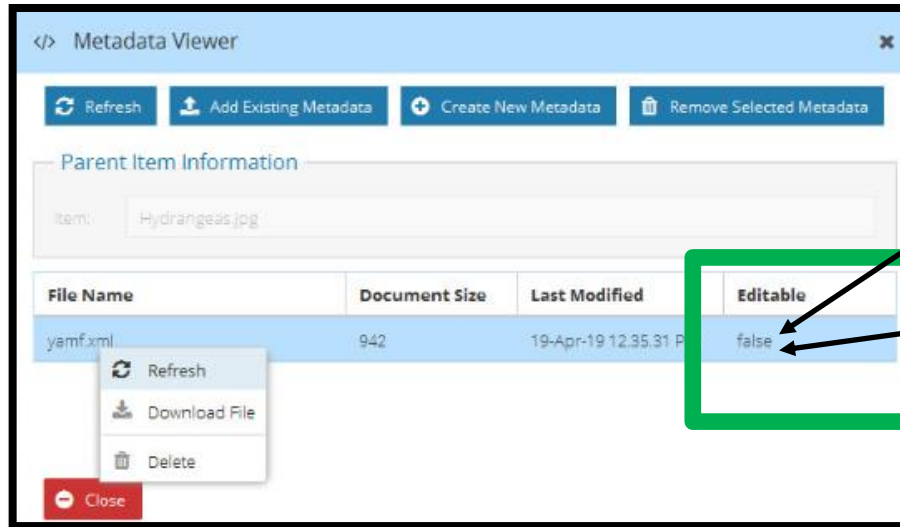


The screenshot shows the 'Metadata Editor' form. It has a title bar 'Metadata Editor' and a close button. The form contains a 'Metadata File Name:' field with a text input. Below this are several sections, each with a plus icon and a label: 'MetacardInfo', 'Resource Identifier', 'Title', 'Contact Info', and 'Subject Coverage'. At the bottom of the form are 'Cancel' and 'Save' buttons.

- Fill out the Metadata Creator Form
- Press Save
- The .XML Metadata file is downloaded to your computer

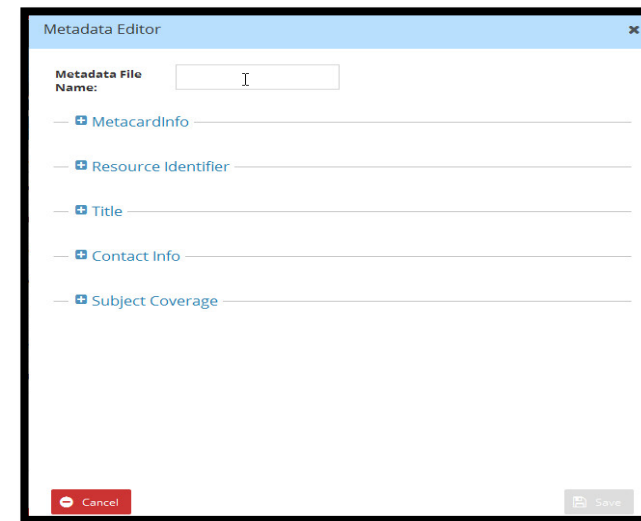
5. Edit Metadata

- If the Metadata was created using the Web's Metadata Creator, then it can be edited in the Metadata Creator too
- After editing, Press Upload.



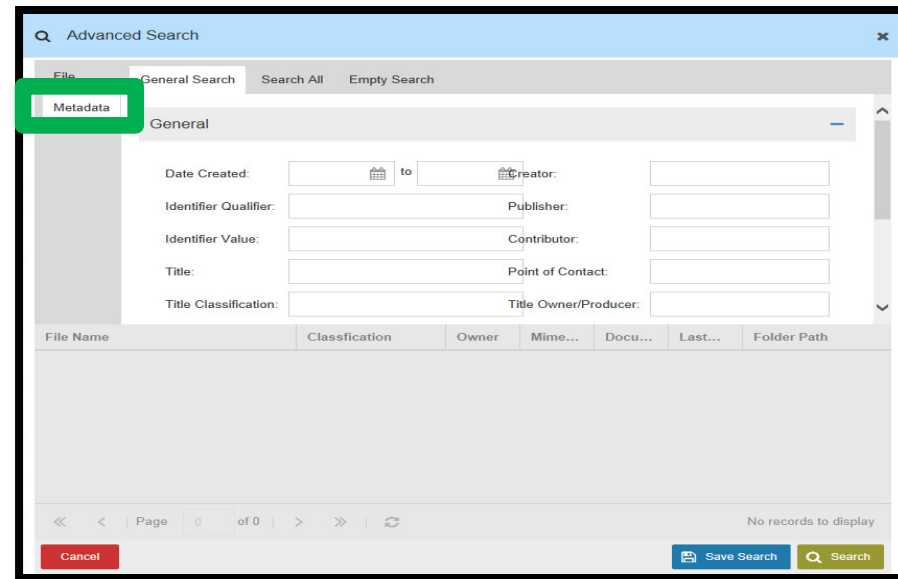
FALSE: Metadata was not created using the Web's Metadata Creator, and therefore cannot be opened in the Metadata Creator

TRUE: Metadata Creator used to create the metadata, and therefore it can be viewed/edited in the Metadata Creator



6. Search Metadata

- Use the Advanced Search screen → Select Metadata
 - DDMS v5.0 has a very large number of fields ; the search form does not have all the DDMS v5.0 fields on it
 - Allows for searching all of the fields on the Metadata Creator form (corresponds to the “header” portion of DDMS v5.0)
- ❖ Search Results are matching the metadata .XML files



The screenshot shows the 'Advanced Search' window. The 'Metadata' tab is selected and highlighted with a green box. The 'General' section contains the following fields:

Field	Value
Date Created:	[Calendar icon] to [Calendar icon]
Identifier Qualifier:	[Text box]
Identifier Value:	[Text box]
Title:	[Text box]
Title Classification:	[Text box]
Creator:	[Text box]
Publisher:	[Text box]
Contributor:	[Text box]
Point of Contact:	[Text box]
Title Owner/Producer:	[Text box]

Below the fields is a table with the following headers: File Name, Classification, Owner, Mime..., Docu..., Last..., Folder Path. The table is currently empty. At the bottom, there is a 'Cancel' button, a 'Save Search' button, and a 'Search' button. The status bar indicates 'No records to display'.

Search Metadata for Files/Folders



1. Use the Advanced Search screen → Select *Metadata*
2. Enter search criteria in the desired metadata field(s)
3. Return to the File Search
4. Enter File Search criteria if desired
5. Select *Files & Folders* in the Search results. Press *Search*.

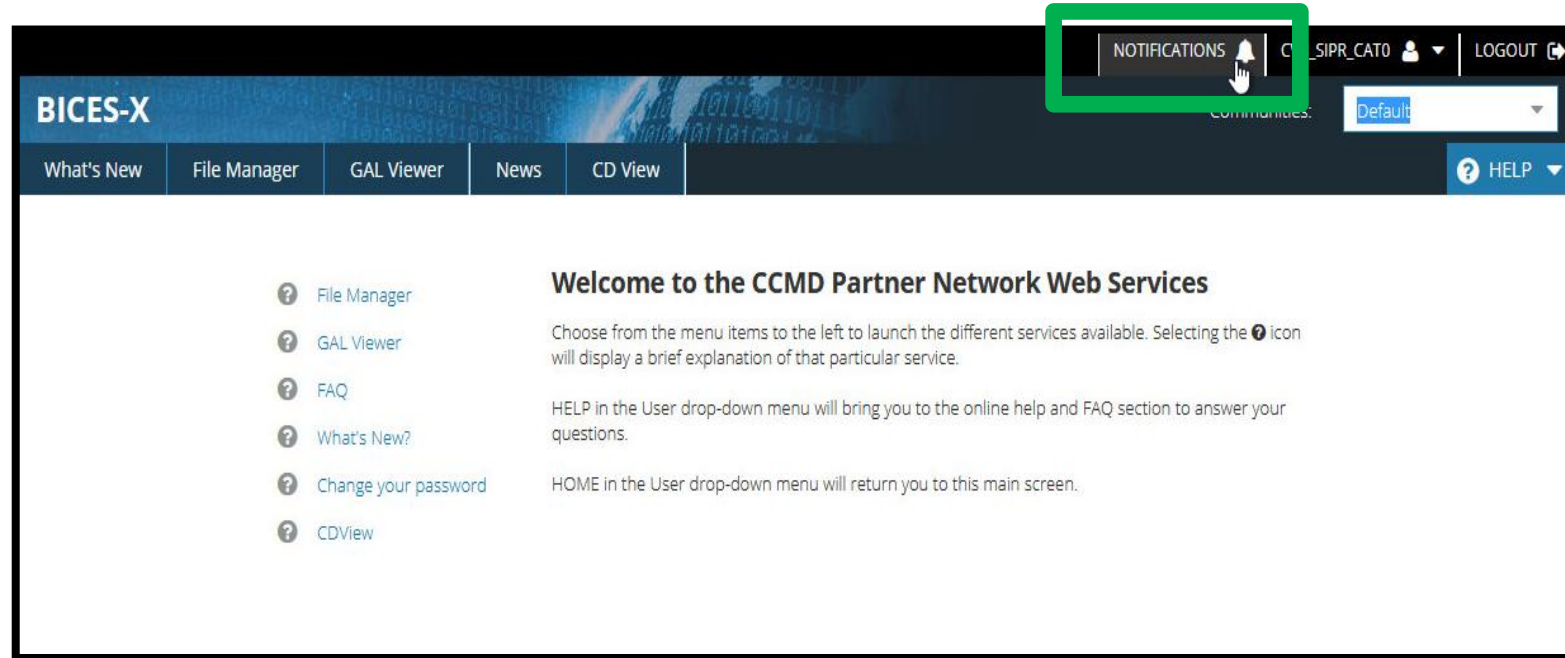
❖ Search Results are matching the metadata .XML files

A screenshot of the 'Advanced Search' web application. The 'File' tab is highlighted with a green box. The 'Metadata' section is expanded, showing various search fields such as 'Date Created', 'Identifier Qualifier', 'Identifier Value', 'Title', 'Title Classification', 'Creator', 'Publisher', 'Contributor', 'Point of Contact', and 'Title Owner/Producer'. Below these fields is a table with columns for 'File Name', 'Classification', 'Owner', 'Mime...', 'Docu...', 'Last...', and 'Folder Path'. The table is currently empty, and the status at the bottom indicates 'No records to display'. Navigation buttons like 'Cancel', 'Save Search', and 'Search' are visible at the bottom.

UNCLASSIFIED

Notifications

- TNE 12S Web can generate notifications to individual users about important events
 - Password expiration impending (starts 20 days prior to the 60-day expiration time period)
 - File upload success ; awaiting acceptance prior to being published
 - File upload failure
- A notification is only for one user, and cannot be shared or seen by other users



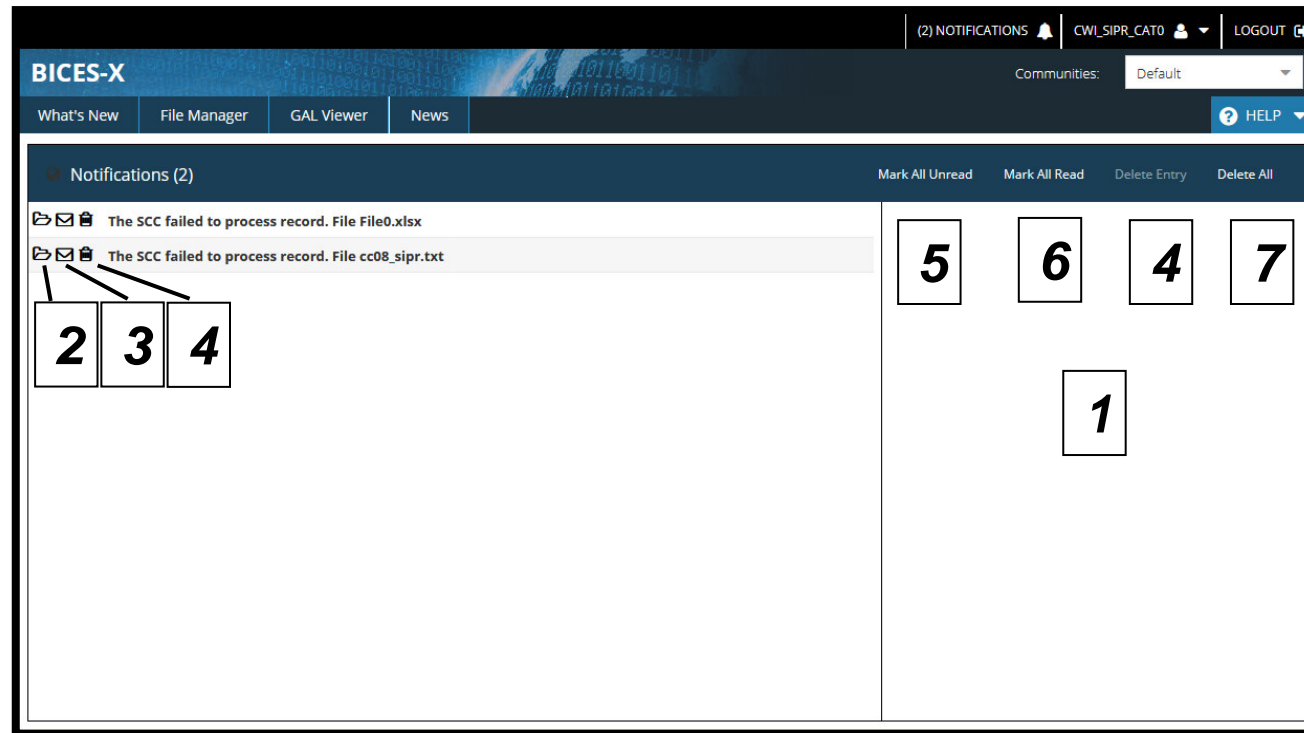
Notifications



Notifications Auto-expire after 7 days, unless the user “Saved” the notification

Notification actions:

1. View detailed information
2. Save & un-save notification
3. Mark Read/Un-read
4. Delete notification
5. Mark All Unread
6. Mark All Read
7. Delete All

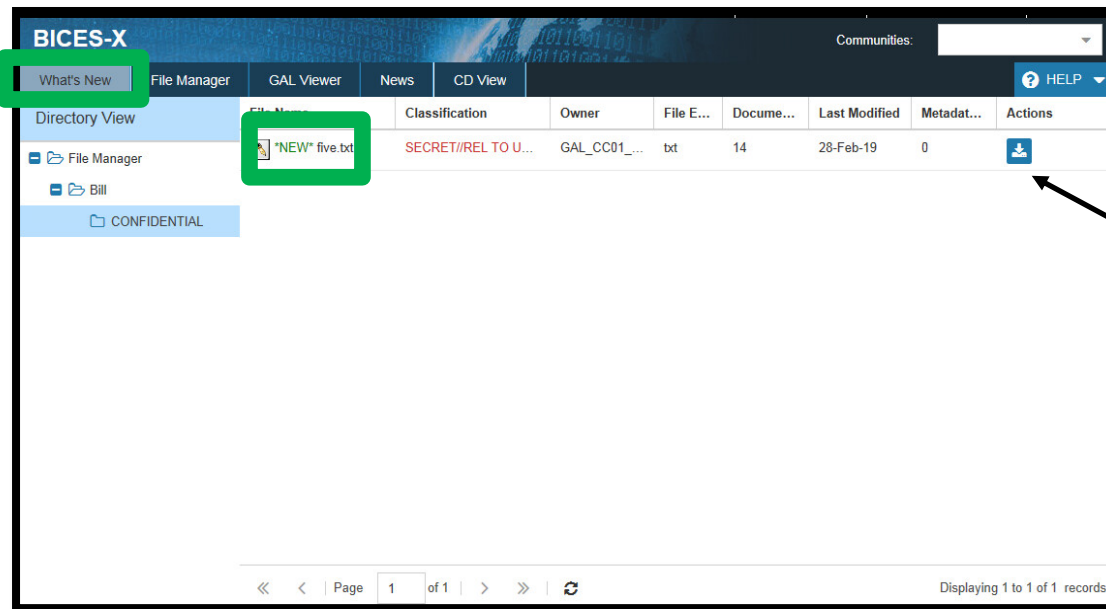


UNCLASSIFIED

What's New?



- Three ways of discovering new content (only for content that you are allowed to see)
 1. (Same as Release 3.0) Use the Advanced Search screen to search by Date Range
 2. “What’s New?” screen Displays Files and Folders which are new within the last 24 hours
 3. Or, a *NEW* signifier can be seen in the File Manager, next to files and folders which are new within the last 24 hours
- **Changes** to **existing** files & folders don’t show up as “New”
 - ❖ Such as folder name change or folder re-label



The only action allowed on the “What’s New?” screen is file download





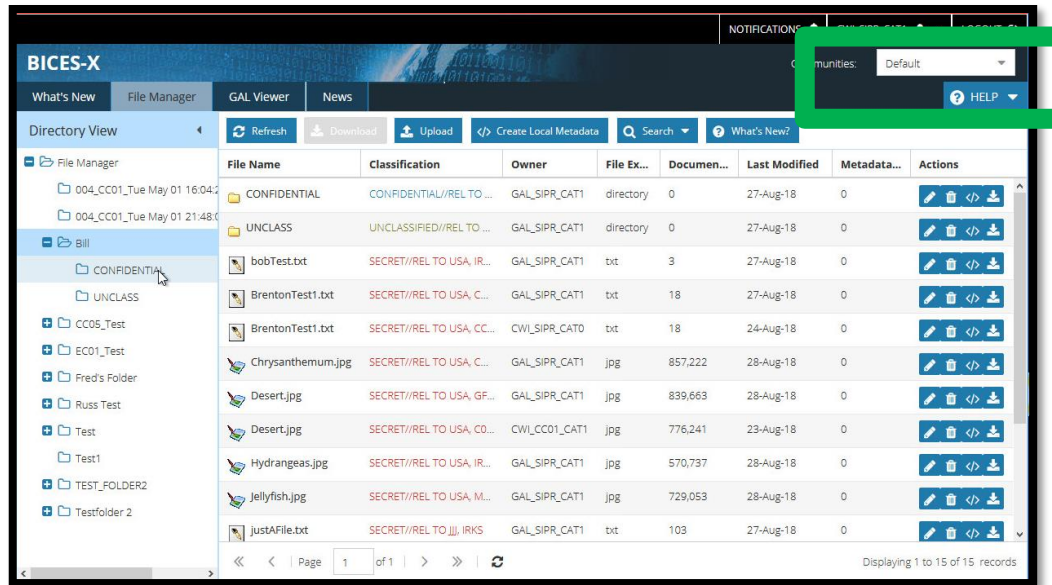
Restricted Communities

- This feature is invisible to you, unless enabled by a Web Administrator
- If you need to use it, you'll know, because someone will tell you
- So, what is it?
 - A Restricted Community is a “sandbox” within which files & folders are held
 - It can be thought of as a new root folder
 - All existing files and folders are now in a Restricted Community called “Default”
 - All existing user accounts are member of the “Default” Restricted Community
 - New user accounts are added to “Default” Restricted Community, unless there are special circumstances
 - Only members of a Restricted Community can see files & folders in that Restricted Community
 - A file and folder can only be a member of **one** Restricted Community



Restricted Communities

- A “virtual sandbox” where all the files, folders, and metadata resides
- A user can be a member of multiple Restricted Communities
- Restricted Communities can be created or removed by Web Administrators
- Users can be added to or removed from Restricted Communities by Web Administrators
- How to switch between which Restricted Community you are viewing
 - View one at a time only!



When you upload a file, it goes into the selected Restricted Community

The File Manager only shows you the files, folders, metadata in the selected Restricted Community



- What is TNE?
- Account Request
- Email
- Voice
- Chat
- File Share
- Email and File Share Rejection Fixes
- Points of Contact





Support & Points of Contact

UNCLASSIFIED

Coalition Support Service Desk (CSSD) – Help Desk 24/7

Phone: +44-1480-84-2815/2816

BICES Phone: 0013112000

Phone DSN: (314) 268-2815/2816

BICES:coalitionsupport@usa.bices.org

Virtual Networks Operations – (VNOSC) 24/7

BICES Phone: 0015002600

Phone: (813) 826-1693





OVERALL CLASSIFICATION: UNCLASSIFIED

CONNECTS THE COALITION

QUESTIONS?

UNCLASSIFIED