General Policies

IMCOM Enterprise Web

Tutorial 10

Version 2.6

Standard Operating Procedures

Contents and general instructions

PAGE:

3. Controlling documentation and guidance
4. Introduction: Moderate-Impact System
5. Introduction: IEW Impact level
6. Procedures: Log out
7. Requirements: Clearances
8. Roles in IMCOM Enterprise Web
9. Roles at the Garrison
10. Minimum training requirements for contributors
11. IEW Training and Resources
12. Credentialing contributors
13. Account policies
14. Access to personal information
15. Rescinding and Revoking accounts
16. Double-checking (validation and revalidation) of personal information
17. Requirement: Maintaining records
18. Requirement: Quarterly local audit
19. Requirements: Accounts
20. Requirements: Passwords /Pass Phrases ●
21. OPSEC Level II
22. Naming convention for home.army.mil
23. Data Mining
24. Logging and auditing
25. Guest access and mobile devices policy
26. Links policy
27. Forms: References, definitions and scope
28. Forms: Order of preference and general rules
29. Forms: Privacy Considerations
30. Forms: Privacy and Data Integrity
31. Forms: Preauthorized and existing forms
32. Forms: Making downloadable and web forms
33. Forms: Contact Us
34. Forms: Nonconforming forms
35. Updating your signature

General instructions:

This document sets forth policies IEW users must agree to for access to the system. All should be considered official. For questions or to request exceptions, please contact IMCOM HQ PAO.
These policies help IEW conform to national and DOD cyber security regulations. The previous version added a section on forms. This version adds a page dedicated to passwords.

IMCOM Enterprise Web documentation can be found on IEW Pro Central,
https://homeadmin.army.mil/imcom/index.php/contact/webmaster-1/pro-central
These tutorials also serve as SOP for IMCOM Enterprise Web.

IMCOM GUIDELINES:
The dark gray boxes are policy reminders.

Blue boxes offer helpful explanations

NEW! ● <-- added or substantially new since last version

NEW!

Controlling documentation and guidance

IMCOM Enterprise Web is controlled by the following documents:

- IMCOM Web Policy
- Tutorials 1-10, comprising the SOP for the system
- Tiered Menu Layout

These documents are available on a library page under the IMCOM HQ Webmaster site. They are also distributed to the IEW mailing list annually or after major updates.

- Operations Manual: This contains the Access Control Plan, Privacy Protection Plan, Site Security Plan, and other in-depth instructions for policy and execution.

Introduction: Moderate-Impact System

- **Potential Impact** [FIPS 199] The loss of confidentiality, integrity, or availability could be expected to have: (i) a *limited* adverse effect (FIPS Publication 199 low); (ii) a *serious* adverse effect (FIPS Publication 199 moderate); or (iii) a *severe* or *catastrophic* adverse effect (FIPS Publication 199 high) on organizational operations, organizational assets, or individuals.
- **Confidentiality** [44 U.S.C., Sec. 3542] Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
- **Integrity** [44 U.S.C., Sec. 3542] Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.
- **Availability** [44 U.S.C., Sec. 3542] Ensuring timely and reliable access to and use of information.
- **Moderate-Impact System** [FIPS 200] An information system in which one of the three security objectives (i.e., confidentiality, integrity, and availability) is assigned a FIPS Publication 199 potential impact value of moderate.

Introduction: IEW Impact level

IMCOM Enterprise Web Impact Categorization	
Confidentiality	Moderate
Integrity	Moderate
Availability	Moderate

SYSTEM CONFIDENTIALITY LEVEL	
Unclassified Public	**System stores <u>Unclassified information</u> approved for public release.**

Other Information Classes	
Definition	Present
Controlled Unclassified Information (CUI)	**No**
Privacy Act data, such as Social Security Number	**YES***
Health Insurance Portability and Accountability Act (HIPAA)	**No**
DOD financial (budget) data	**No**
DOD critical operation data	**No**
DOD administrative data	**No**
COTS proprietary data	**No**

Reference NIST 800-60 vol. 2), the overall FIPS 199 categorization for IEW is Low. In order to ensure the appropriate controls were identified for implementation commensurate with an overall Low, Low, Low rating for IEW, the IEW Package was created in eMASS with the appropriate overlays for a confidentiality, integrity & availability categorization of Low. eMASS identified 310 applicable controls based on NIST SP 800-53 R.4.
Risk Assessments are to be accomplished on an annual basis.

*IEW DOES NOT store Social Security numbers. However, some Privacy Act data are collected under controlled circumstances: Names and private and professional addresses, phone numbers and email addresses

Procedures: Log out

- Log out of IEW when you are finished with your session or at the end of your official work period. Do not leave the window open on your desktop outside duty hours.

Requirements: Clearances

- **Garrison Manager, Site Manager and Page Manager must have *DoD Final SECRET* security clearance, or at minimum an *Interim Secret* while their clearance paperwork is being processed and they are waiting on the final clearance decision/determination.**
- Privileges assigned to Garrison Managers are reviewed at least annually to validate the need for such privileges.

Roles in IMCOM Enterprise Web

Role	Assigns membership to these groups / accounts	Authorized to create temporary accounts	Clearance	Account Type	Concrete5 account name	Documentation required	Overview
System Administrator		Authorized to create temporary accounts	Secret	System Administrator		SAAR/PAA	Access to data center. Performs the highest-privilege system administration and environment configuration
Database Administrator			Secret	Database Administrator		SAAR/PAA	Access to data center. Database administrator that manages structure and access to CSD-RMF databases
Information System Security Officer (ISSO)		Authorized to create temporary accounts	Secret	Information System Security Officer (ISSO)		SAAR/PAA	Security functions, e.g. audit log review
CMS Administrator	Garrison Manager, Site manager	Authorized to create temporary accounts	Secret	CMS Manager	imcom	SAAR/PAA	Access to application, limited access to data center. Manages the Concrete5 application and controls access for end users (Garrison and site Managers and contributors)
Garrison Manager	Page Manager, Page Contributors, Text Editors	Authorized to create temporary accounts on the garrison site	Secret	Garrison Manager	Garrison Manager	SAAR	Access to application (end user). Manages content, access and privileges within a garrison site. Granted additional permission on a case-by-case basis. *Typically garrison PAO or NEC*
Site Manager	Page Manager, Page Contributors, Text Editors	Authorized to create temporary accounts on the garrison site	Secret	Site Manager	Site Manager	SAAR	Access to application (end user). Manages content, access and privileges within a garrison site. *Typically garrison PAO or NEC*
Page Manager			Secret	Page Manager	Page Manager	SAAR	Access to application (end user). Manages content and occasionally access within a section of a garrison site. *Tenant PAOs, Directorates with publishing authority*
Page Contributor			None	Page Contributor	Page Contributor	SAAR	Access to application (end user) Edits content within a garrison site without publishing priviliges. *Editors within a tenant or directorate.*
Text Editor		Authorized to add very specific content	None	Text Editor	Text Editor	SAAR	Access to a page or editable area. No publishing privileges. *Editors within a tenant or directorate.*
General Public			None	None	None		View public information
Foreign National			None	Foreign National		SAAR	Limited access to authorized information
Contract Employee			None	Contract Employee		SAAR	Limited access to authorized information

Roles at the Garrison

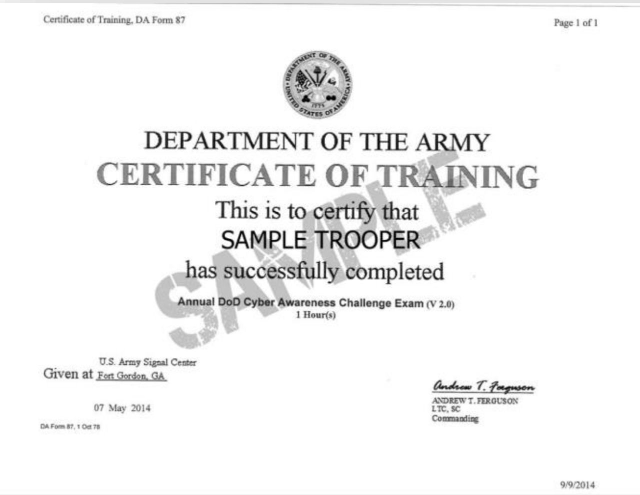
- **Garrison Manager, or Garrison Web Manager:**
  - Chief point of contact for the IMCOM Enterprise Web at the garrison. When the garrison is responsible for something, this is the first person on the call list. Otherwise, the person has the same responsibilities as a Site Manager.
  - Training requirements: Must be public affairs qualified (hold a GS-1035 or 1082 designation, or a 46 A or Z MOS) or hold an OPSEC Level II certificate (during the transition to these new requirements, the GM, SM, or PM can substitute the online Web Content and OPSEC Training Course as long as they actively seek OPSEC Level II as soon as it is available).Responsible for knowing contents of the Tutorial/SOPs.
- **Site Manager:**
  - A member of the website team at the installation, with authority and permission to edit any item in the system. If there is more than one site manager, a Garrison Manager should be appointed.
  - Training requirements: Must be public affairs qualified (hold a GS-1035 or 1082 designation, or a 46 A or Z MOS) or hold an OPSEC Level II certificate (during the transition to these new requirements, the GM, SM, or PM can substitute the online Web Content and OPSEC Training Course as long as they actively seek OPSEC Level II as soon as it is available). Responsible for knowing contents of the Tutorial/SOPs.
- **Page Manager:**
  - A person designated to manage a subsection of the garrison site, such as a directorate, tenant or senior command site. The Page Manager has publishing privileges within his or her subsite.
  - Training requirements: Must be public affairs qualified (hold a GS-1035 or 1082 designation, or a 46 A or Z MOS) or hold an OPSEC Level II certificate (during the transition to these new requirements, the GM, SM, or PM can substitute the online Web Content and OPSEC Training Course as long as they actively seek OPSEC Level II as soon as it is available).
- **Page Contributor:**
  - A person designated to work on, perhaps manage, a subsection of the garrison site. The Page Contributor can add and remove pages within the section, but CANNOT publish.
  - Training: Requires Web Content and OPSEC Training Course.
- **Text Contributor (formerly Text Editor):**
  - Appointed to manage a single block or limited copy on a page. Must be supervised/reviewed by a Site or Page Manager.

Minimum training requirements for contributors

IMCOM GUIDELINES:
To protect the operations security of the IMCOM Enterprise Web, every person allowed to log on must have at a minimum an up-to-date Cyber Awareness Challenge certificate. Page Managers and Page Contributors must also have a current certificate from the Web Content and OPSEC Traning Course. Those granted publishing rights (Page Managers and Site Managers) must also have either OPSEC Level II certification or have a Public Affairs career designation (CP-22/MOS 46A or Z.

Garrisons may add their own restrictions to these minimum guidelines.

Garrison Managers will keep certifications on file for periodic review and send copies to the CMS Manger at IMCOM HQ PAO.



Certificate of Training, DA Form 87

Page 1 of 1

DEPARTMENT OF THE ARMY

CERTIFICATE OF TRAINING

This is to certify that

SAMPLE TROOPER

has successfully completed

Annual DoD Cyber Awareness Challenge Exam (V 2.0)

1 Hour(s)

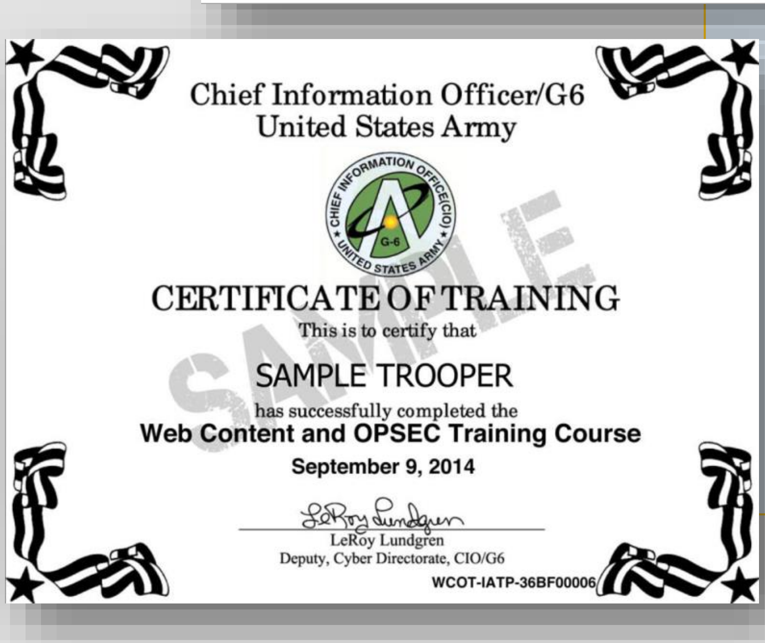
Given at U.S. Army Signal Center
Fort Gordon, GA

07 May 2014

Andrew T. Ferguson
ANDREW T. FERGUSON
LTC, SC
Commanding

DA Form 87, 1 Oct 78

9/9/2014



Chief Information Officer/G6
United States Army

CERTIFICATE OF TRAINING

This is to certify that

SAMPLE TROOPER

has successfully completed the

Web Content and OPSEC Training Course

September 9, 2014

LeRoy Lundgren
LeRoy Lundgren
Deputy, Cyber Directorate, CIO/G6

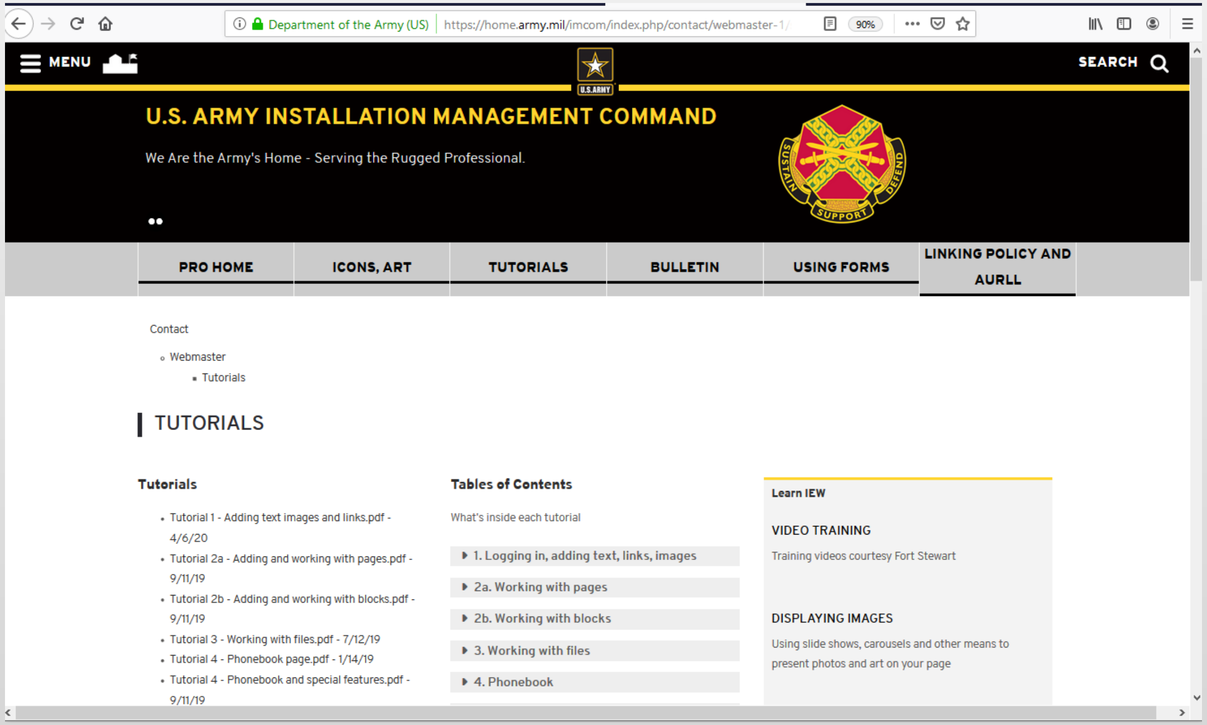
WCOT-IATP-36BF00006

DoD Cyber Awareness Challenge Training (URL - https://ia.signal.army.mil/)
Complete Step 1: “DOD Cyber Awareness Challenge” then Step 2: Army Required Exam
1. Click Log in with CAC DoD-Approved Certificate Login
2. Update record
3. Select “DOD Cyber Awareness Challenge” to review the coursework.
3. Click Take Exam
4. Click Annual DoD Cyber Awareness Challenge Exam (must receive a 70 to receive certificate).

Web Content & OPSEC Training (URL- https://iatraining.us.army.mil/index.html)
The Web Content and OPSEC Certificatinon Training contains four lessons: a Web Content and OPSEC Intro Lesson, a DoD Web Guidance, a Web Content and OPSEC Lesson, and an Army Webmaster test. To receive the Certificate of Training for the Web Content and OPSEC Certification Training, students must take and pass two end-of-lesson tests and the final interactive Webmaster test (must receive a 70 to receive certificate).

NEW!

IEW Training and Resources



U.S. ARMY INSTALLATION MANAGEMENT COMMAND

We Are the Army's Home - Serving the Rugged Professional.

Contact

- Webmaster
  - Tutorials

TUTORIALS

Tutorials

- Tutorial 1 - Adding text images and links.pdf - 4/6/20
- Tutorial 2a - Adding and working with pages.pdf - 9/11/19
- Tutorial 2b - Adding and working with blocks.pdf - 9/11/19
- Tutorial 3 - Working with files.pdf - 7/12/19
- Tutorial 4 - Phonebook page.pdf - 1/14/19
- Tutorial 4 - Phonebook and special features.pdf - 9/11/19

Tables of Contents

What's inside each tutorial

- 1. Logging in, adding text, links, images
- 2a. Working with pages
- 2b. Working with blocks
- 3. Working with files
- 4. Phonebook

Learn IEW

VIDEO TRAINING

Training videos courtesy Fort Stewart

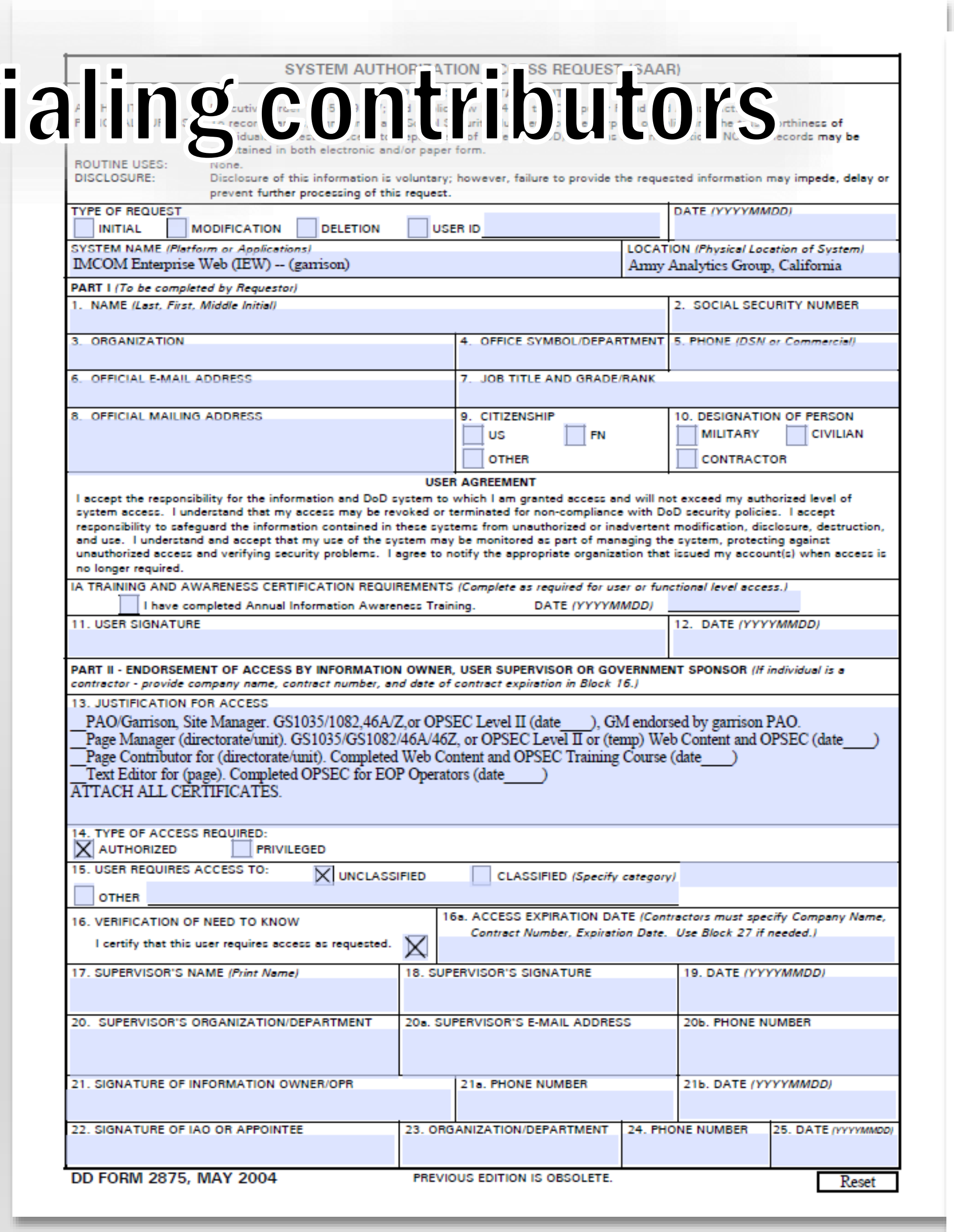
DISPLAYING IMAGES

Using slide shows, carousels and other means to present photos and art on your page

- Check out the resources at https://homeadmin.army.mil/imcom/index.php/contact/webmaster-1/pro-central
- Users are expected to follow a sequential set of tutorials to gain a thorough knowledge of the system. They can also partake of a series of videos (hosted by Fort Stewart YouTube account) covering practically every aspect of using the system. In addition, regular training and updates are provided via teleconference.
- In combination with the video https://www.youtube.com/watch?v=mLjvlHF_hjw, Tutorials 1 and 2 are designed to give page contributors the knowledge they need to make changes within the scope of their responsibility.
- Installations expecting large numbers of contributors may find it helpful to set up formal training.
- Groups of four or more can apply for training workshops led by IMCOM HQ staff.

Credentialing contributors

IMCOM standard: Fill out and keep a 2875 for each person logged into the system. Use your local IA assets for blocks 22-25. Model overlay forms are/will be downloadable from home.army.mil



SYSTEM AUTHORIZATION ACCESS REQUEST (SAAR)

...orthiness of ...records may be ...tained 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 □ INITIAL □ MODIFICATION □ DELETION □ USER ID ____ DATE *(YYYYMMDD)*

SYSTEM NAME *(Platform or Applications)*: IMCOM Enterprise Web (IEW) -- (garrison)

LOCATION *(Physical Location of System)*: Army Analytics Group, California

PART I *(To be completed by Requestor)*

1. NAME *(Last, First, Middle Initial)*

2. SOCIAL SECURITY NUMBER

3. ORGANIZATION

4. OFFICE SYMBOL/DEPARTMENT

5. PHONE *(DSN or Commercial)*

6. OFFICIAL E-MAIL ADDRESS

7. JOB TITLE AND GRADE/RANK

8. OFFICIAL MAILING ADDRESS

9. CITIZENSHIP □ US □ FN □ OTHER

10. DESIGNATION OF PERSON □ MILITARY □ CIVILIAN □ CONTRACTOR

USER AGREEMENT

I accept the responsibility for the information and DoD system to which I am granted access and will not exceed my authorized level of system access. I understand that my access may be revoked or terminated for non-compliance with DoD security policies. I accept responsibility to safeguard the information contained in these systems from unauthorized or inadvertent modification, disclosure, destruction, and use. I understand and accept that my use of the system may be monitored as part of managing the system, protecting against unauthorized access and verifying security problems. I agree to notify the appropriate organization that issued my account(s) when access is no longer required.

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

__PAO/Garrison, Site Manager. GS1035/1082,46A/Z,or OPSEC Level II (date____), GM endorsed by garrison PAO.
__Page Manager (directorate/unit). GS1035/GS1082/46A/46Z, or OPSEC Level II or (temp) Web Content and OPSEC (date____)
__Page Contributor for (directorate/unit). Completed Web Content and OPSEC Training Course (date____)
__Text Editor for (page). Completed OPSEC for EOP Operators (date____)
ATTACH ALL CERTIFICATES.

14. TYPE OF ACCESS REQUIRED: ☒ AUTHORIZED □ PRIVILEGED

15. USER REQUIRES ACCESS TO: ☒ UNCLASSIFIED □ CLASSIFIED *(Specify category)* □ OTHER

16. VERIFICATION OF NEED TO KNOW — I certify that this user requires access as requested. ☒

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)*

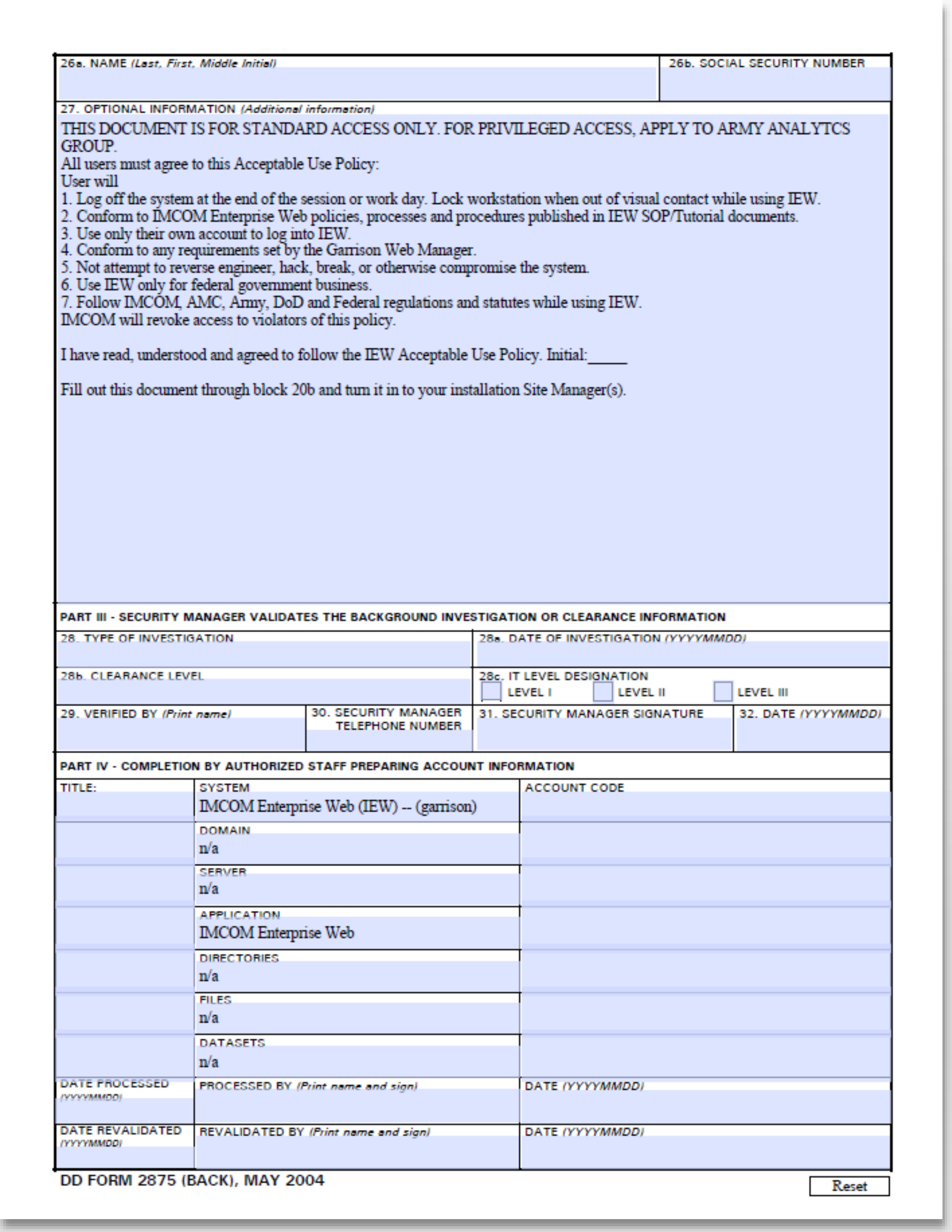
22. SIGNATURE OF IAO OR APPOINTEE

23. ORGANIZATION/DEPARTMENT

24. PHONE NUMBER

25. DATE *(YYYYMMDD)*

DD FORM 2875, MAY 2004 PREVIOUS EDITION IS OBSOLETE. Reset



26a. NAME *(Last, First, Middle Initial)*

26b. SOCIAL SECURITY NUMBER

27. OPTIONAL INFORMATION *(Additional information)*

THIS DOCUMENT IS FOR STANDARD ACCESS ONLY. FOR PRIVILEGED ACCESS, APPLY TO ARMY ANALYTCS GROUP.
All users must agree to this Acceptable Use Policy:
User will
1. Log off the system at the end of the session or work day. Lock workstation when out of visual contact while using IEW.
2. Conform to IMCOM Enterprise Web policies, processes and procedures published in IEW SOP/Tutorial documents.
3. Use only their own account to log into IEW.
4. Conform to any requirements set by the Garrison Web Manager.
5. Not attempt to reverse engineer, hack, break, or otherwise compromise the system.
6. Use IEW only for federal government business.
7. Follow IMCOM, AMC, Army, DoD and Federal regulations and statutes while using IEW.
IMCOM will revoke access to violators of this policy.

I have read, understood and agreed to follow the IEW Acceptable Use Policy. Initial:____

Fill out this document through block 20b and turn it in to your installation Site Manager(s).

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: IMCOM Enterprise Web (IEW) -- (garrison)

ACCOUNT CODE

DOMAIN: n/a

SERVER: n/a

APPLICATION: IMCOM Enterprise Web

DIRECTORIES: n/a

FILES: n/a

DATASETS: n/a

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), MAY 2004 Reset

NEW! Account policies

IMCOM POLICY

When you set up a page contributor or manager account

- Accounts should have an expiration date
- No group/shared accounts are allowed. If more than one person in an office needs access to your web page, each person will have his/her own account.

NEW!

Access to personal information

- All users, from guest to Garrison Manager level, can review and request modification or deletion of any record of information pertaining to themselves on request. This includes mentions in articles and photographs.
- To review, an individual must apply to the Garrison Manager on the installation. The Garrison Manager will confirm the identity of the individual, usually by asking for a photo ID. When the Garrison Manager is satisfied with the individual’s identity, he/she will discuss the record, its use and whether it should be modified or removed.
- The Garrison Manager will keep a record of each individual request and its resolution.

Rescinding and Revoking accounts

- **Rescinding Privileged User Account Credentials**
- Whenever a privileged user account on the IEW system is no longer appropriate or needed the following four (4) steps to disable or revoke the account shall be carried out:
- The privileged user account credentials will be disabled or revoked immediately,
- All shared system/application passwords the privileged user account had access to shall be changed immediately,
- For audit trail documentation the privileged user account holder’s technical lead will forward confirmation to the IEW ISSO that the credentials have been disabled or revoked.
- **Emergency revocation of User Account Credentials**
- Accounts can be revoked immediately, when required, by the ISSO, PAO or Branch Chief.

NEW! Double-checking (validation and revalidation) of personal information

- Every online form collecting PII should have the following near the submit button: “Please review your information and correct any errors before submitting.”
- Confirm the information on initial and subsequent contacts by direct questioning (“I have your email as crankycivilian@beatit.com. Is that still correct?”

Requirement: Maintaining records

- Garrison managers must maintain the following records electronically:
- SAARs for current and past account holders
- A list of individuals by role/account, account creation date, training date and expiration/renewal date.
- Any notes related to the disabling or removal of accounts for reasons other than expiration or leaving the role.
- Records of quarterly audit reviews.

Requirement: Quarterly local audit

- The Garrison Manager (or designated Site Manger if no Garrison Manager is identified) must take the time every three months to
  - Look at every page on the site.
  - Scan the log
- Record:
  - Date(s) of the review
  - Any unauthorized content and what was done about it.
    - Nonpublic information
    - PII and HIPA violations
    - OPSEC compromises
  - An affirmation that the website is clear of potential violations.

Requirements: Accounts

- Accounts should have an expiration date no later than 1 year after creation.
- No group/shared accounts are allowed.
- Passwords will not be shared.
- If you discover or find out about an account being used in a risky manner (OPSEC, cybersecurity, PII violations), disable it immediately and contact <<TO COME: A GROUP MAILBOX FOR CONTACTING BOTH IMCOM PAO AND THE ISSO AT AAG>>
- Passwords or passphrases must 15-256 characters long. They must contain a mix of upper case letters, lower case letters and numbers and may include special characters. No personal information -- names, phone numbers, account names -- or dictionary words. Do not reuse any previous 10 passwords.
- Logon attempts are limited to three failures, which will result in the account being locked out for a set amount of time.

NEW!

Requirements: Passwords /Pass Phrases

```
0pUn5esame?Rlly?!
^^^^^^^^^^^^^^^
```

```
^^^^^^^^^^^^^^^^^^^^
^^^^^^^^^^^^^^^^^^^^
^^^^^^^^^^^^^^^^^^^^
^^^^^^^^^^^^^^^^^^^^
^^^^^^^^^^^^^^^^^^^^
^^^^^^^^^^^^^^^^^^^^
^^^^^^^^^^^^^^^^^^^^
^^^^^^^^^^^^^^^^^^^^
^^^^^^^^^^^^^^^^^^^^
^^^^^^^^^^^^^^^^^^^^
^^^^^^^^^^^^^^^^^^^^
^^^^^^^^^^^^^^^^^^^^
^^^^^^^^^^^^^^^^
```

IEW is protected by the NIPR-firewall. Using your CAC to log in to your computer protects IEW. The uneditable home.army.mil sites are available to the public, while the editable homeadmin.army.mil are not. This allows us to use passwords to log in from the NIPR. However, they must still be standards-compliant.

IMCOM GUIDELINES:

Passwords or passphrases must

- Be 15-256 characters long
- Contain at least two
  - upper case letters,
  - lower case letters
  - Numbers
  - special characters.
- Be free pf personal information -- names, phone numbers, account names –
- Not use dictionary words.
- Be at least 50 percent new
- Do not reuse any previous 10 passwords.
- Be changed every 60 days
- Not be changed more than once every 24 hours

Based on DISA's "Application Security and Development STIG, V3R2", section 3.1.24.2, and National Institute of Standards and Technology Special Publication 800-63B

The draft DISA standard is higher than the standard published in eMASS
The information system, for password-based authentication:
(a) Enforces minimum password complexity of [As supported by the device: minimum of 15 Characters, 1 of each of the following character sets: - Upper-case - Lower-case - Numerics - Special characters (e.g. ~ ! @ # $ % ^ & * ( ) _ + = - ‘ [ ] / ? > <)];];
(b) Enforces at least the following number of changed characters when new passwords are created: [As supported by the device: 50% of the minimum password length];
(c) Stores and transmits only cryptographically-protected passwords;
(d) Enforces password minimum and maximum lifetime restrictions of [As supported by the device: minimum 24 hours, maximum 60 days];

- (e) Prohibits password reuse for [As supported by the device, minimum of 5.] generations; and
- (f) Allows the use of a temporary password for system logons with an immediate change to a permanent password.

OPSEC Level II

- At least one member of the Web management team (or the PAO) must be OPSEC Level 2 Certified. Public Affairs professionals with release authority (usually the PAO or the PA NCO) have had enough training in OPSEC to substitute for a certificate holder

Naming convention for home.army.mil

- All Enterprise Web sites follow the same naming convention:
- https://home.army.mil/(garrisonname)
- If there is some high-level reason to go with another garrison name, we might be able to do it. But the reason can't be a matter of taste or temporary priorities (hence, no home.army.mil/risingsun). If it causes friction with the host nation or confusion of some kind, we'll entertain a change.
- Fort, USAG, ASA, JB are typically left out

Data Mining

Data mining as an analytical process that attempts to find correlations or patterns in large data sets for the purpose of data or knowledge discovery.

- Attempts to mine data from IEW are discouraged.
- First, most information collected by IEW is protected by privacy regulations and must be used only in ways specifically spelled out in privacy advisories on the page. Second, IEW doesn't collect that much data. Third, many, many regulations govern the process.
- Any activity intending to mine data from IEW must provide the following to IMCOM headquarters:
- A thorough description of the data mining activity, its goals and, where appropriate, the target dates for the deployment of the data mining activity.
- A thorough description of the data mining technology that was or will be used, to include the basis for detennination of whether a particular pattern or anomaly was indicative of terrorist or criminal activity.
- A thorough description of the data sources that were used.
- An assessment of the efficacy or likely efficacy of the data mining activity to provide accurate information consistent with and valuable to the stated goals and plans for the data mining activity.
- An assessment of the impact or likely impact of the implementation of the data mining activity on the privacy and civil liberties of individuals, including a thorough description of the actions taken or will be taken with regard to the property, privacy, or other rights or privileges of any individual or individuals as a result of the implementation of the data mining activity.
- A list and analysis of the laws and regulations that govern the information collected, reviewed, gathered, analyzed, or used in conjunction with the data mining activity, to the extent applicable in the context of the data mining activity.
- A thorough discussion of the policies, procedures, and guidelines that are in place or that are to be developed and applied in the use of such data mining activity in order to:
  - Protect the privacy and due process rights of individuals, such as redress procedures; and
  - Ensure that only accurate and complete information is collected, reviewed, gathered, analyzed, or used, and guard against any hannful consequences of potential inaccuracies.

(based upon Secretary of Defense Reports on Federal Data Mining Programs Within the Department of Defense, Fiscal Years 2012 & 2013 and 2014)s

Logging and auditing

- All Site Managers will ensure Login Log is enabled. The Logging function is used to automatically audit account creation, modification, enabling, disabling, and removal actions, and notifies

Guest access and mobile devices policy

- Signed and dated documentation that defines the user actions that can be performed on the information system without identification or authentication consistent with organizational missions/business functions.
- The organization being inspected/assessed establishes and documents usage restrictions for each type of remote access allowed.
- The organization authorizes connection of mobile devices to organizational information systems.

Links policy

Minimize or eliminate links to nongovernmental sites. Monitor the outside sites you link to.

MARK ALL EXTERNAL LINKS. All .com (except for official MWR sites), .org, .edu, .info, dot-whatever should have, at a minimum, an External Link Snippet attached. See Tutorial/SOP 1 for details.

On every page where you use the snippet, include a text line with the snippet and " =Non-Government Link." Link this to our Terms of Use page.

NEW!

Forms: References, definitions and scope

- References:
- AR 25-55, The Department of the Army Freedom of Information Act Program
- AR 25-22, The Army Privacy Program
- AR 25-30, Army Publishing Program, Section 5
- DA Pam 25-40, Army Publishing Program Procedures, Chapter 12
- DoD Instruction 8170.01, Online Information Management and Electronic Messaging
- DoD Instruction 7750.07 DoD Forms Mangaement Program
- DoD Manual 7750.07M, DoD Forms Mangement Program Procedures Manual
- DoD Privacy, Civil Liberties and Transparency Division website
- 1. SCOPE
- This guidance covers all forms on IEW, as defined in DA Pam 25-40, Chapter 12-3
- 12–3. What is a form?
  a. A form is a fixed arrangement of captioned spaces designed for gathering, organizing, and transmitting prescribed information quickly and efficiently. It also serves as a historical record. A form may be in hardcopy, stand-alone electronic file, electronic system of Web based screen(s), or other media. Certificates are forms. Items such as labels, stickers, tags, instruction sheets, notices, and file covers do not require insertion of information; however, they may still be considered forms for procurement purposes.

Forms: Order of preference and general rules

- Both Web forms (those filled in directly on the page) and downloadable/fillable forms (such as .pdfs or Word documents for users to fill out and send in) are covered here.
- **2. ORDER OF PREFERENCE:**
- Follow this order of preference when choosing what kind of form to use:
- a. When they become available: Use one of the preauthorized web forms available from IMCOM Headquarters
- b. Use a suitable, existing SF, OF, DA, DD, AMC or IMCOM form. If necessary, partially fill in the form (overprint) and upload it to your site to be downloaded, filled-in, and returned via email.
- c. Produce an authorized local downloadable form.
- d. Produce a custom web-based fillable form.
- **3. ALL FORMS**
- All forms must be approved by the Forms Mangement Officer (FMO) appropriate to the organization and level. A form issued by the senior command should be signed off by the command's form manager. A copy of the approval should be forwarded to the IEW CMS manager (currently Neal Snyder). The garrison form manager is typically also in charge of privacy, Freedom of Information Act, and document management. As such, they can provide valuable assistance as you build your forms.
- All forms must be prescribed by a regulatory document at the appropriate level. The regulation needs to mention the form by name/number and offer instructions on its use.
- If it's a local form, find a garrison or senior command regulation calling for the use of the form. Office forms should be guided by an SOP or memorandum. When you work with your forms manager, they may be able to affect local regulations or policy to allow you to use the form.
- All forms must include a a privacy act statement or privacy advisory (DoDI 8170.01, DoDI 7750.07). They must be numbered and cataloged.
- All forms must include a reminder to recheck contact information (PII) before sending.

NEW!

Forms: Privacy Considerations

- IEW is authorized to collect and store a limited amount of Personally Identifying Information (PII) under certain conditions. PII is defined and protected by the Privacy Act of 1974.
- Due to the nature of the software, any web-based form will store its information for an indefinite period. This triggers Privacy Act protection.
- IEW can collect name, work and home addresses, work and private phone numbers, work and private email addresses, position, title and rank or grade.
- The purpose of this collection, in general, is to facilitate initial communication between an individual and a garrison agency. It is not to be used for determination of rights, privileges or similar life-altering decisions.
- The garrison user must, on first contact, review and either confirm or correct the individual's information.

NEW!

Forms: Privacy and Data Integrity

- Organizations must take reasonable steps to confirm the accuracy and relevance of PII.
- When you access the information collected in a form and reply via phone, email or direct contact, ask the user to repeat the name, address, email address and phone number (the PII) to ensure they are accurate.
- IEW stores all forms communications in a database. No data should remain in the system longer than 90 days.

NEW!

Forms: Preauthorized and existing forms

- **4. PREAUTHORIZED WEB FORMS**
- We are in the process of producing forms available as blocks that can be dragged and dropped into your site. None are available yet. Once they are complete, you will be able to add them without any additional paperwork. We do have authorization to build the following:
- **Service work order:**
- **Contact Us:**
- **5. EXISTING AGENCY FORMS**
- ***All requirements are met by the publishing agency -- you don't have to go through the authorization process. We will help you pick out, overprint (if necessary) and upload your forms.***
- a. Check for a suitable existing GSA Standard Form (SF), GSA Optional Form (OF), Department of the Army (DA) Form, Department of Defense (DD) form, or IMCOM form (this will be the easiest route), in that order (see the hierarchy on p. 141-142 of DA Pam 25-40). Links to the forms sites are available in the right column.
- --If the form works as-is, consider linking directly to the form on the site, in case of later updates.
- --If you need to partially fill in or customize the form (such as adding a button to send the form by email, you can host it as a downloadable file on IEW.
- --DO NOT upload completed forms (that is, containing PII) to IEW. Instead, set it up to be submitted throuogh Adobe Acrobat to your email address.

Forms: Making downloadable and web forms

- 6. INSTALLATION, LOCAL AND OFFICE FORMS
- If an existing form doesn't fulfill the need, you can work with your FMO to produce a new form. There are two kinds (DA PAM 25-40):
- g. Installation and local forms. These forms are prescribed for use only within a particular headquarters, such as an installation or activity headquarters and are prescribed by an installation regulatory publication for use within the installation. Examples are “Fort Lee Form 1234” and “Redstone Arsenal Form 1234.” ...
  h. Office forms. If a form is used by only one organizational element, such as an office, a prescribing publication is not required; however, appropriate written guidance is recommended (for example, an SOP or office memorandum).
- An office form needs to follow the same Privacy Act and numbering rules as installation or DA forms. For instance, your local model release might need to be named "Fort Notional PAO Form 3" and include a Privacy Act Statement.
- Of course there is a form for this process: DD Form 67*. Use it.
- Seeking form approval is not automatically the job of PAO, garrison G6 or the NEC. The office with an interest in posting the form should take the lead.
- The office requiring the form must work with the forms manager appropriate to their chain of command (garrison offices work with the garrison forms manager) to ensure regulatory compliance (we'll need a note of approval). They will probably simply take the document you use already and put a form number and privacy statement on it. The advantage here is once you work it out, you can collect different PII than IEW will allow you to. If required, the forms manager will work with the requesting office to set up the required privacy controls.
- 7. CUSTOM WEB FORMS
- Web forms are still an option. They must be built here in Texas and , be changed here at headquarters and be approved by the CMS manager (me), AND YOUR LOCAL Privacy office and the Cybersecurity cell. We have locked down editing for web forms we've been able to find and disabled all forms creation tools. I am also working on Privacy Act Statements or Privacy Advisories for those forms that need them.
- Almost all of the rules regarding downloadable forms apply to web-native forms.
- All web forms must include a reminder to recheck contact information (PII) before sending.

Forms: Contact Us

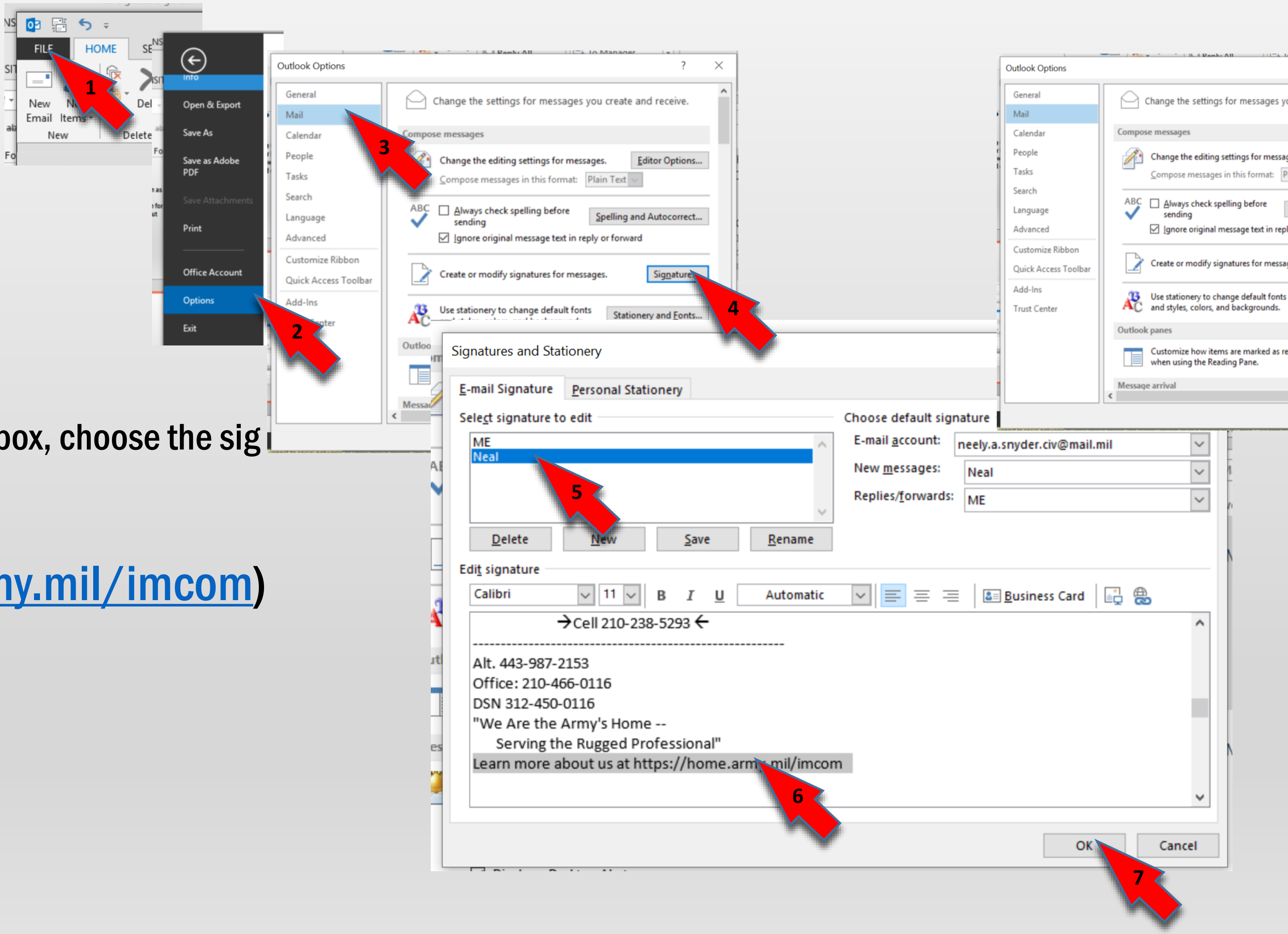
- **8. 'CONTACT US'**
- "Forms" asking for name, email or phone and a message are simple contact instruments. Their purpose is not to organize or store information. Based on a survey of practices across Army and DoD websites, including defense.gov, ARCYBER and HQDA do not use a Privacy Act Statement (PAS) with this kind of instrument. Many do include Privacy Advisories (per DODI 8170.01 3.27). An example is the contact form at the bottom of https://www.defense.gov/Ask-Us/.
- RULES:
- All fields must be optional.
- Do not ask for specific information
- Include a link to the Terms of Service page labeled "Privacy Advisory" as close as possible to the form (our privacy advisory is included in our TOS). All forms must include a reminder to recheck contact information before sending.

NEW!

Forms: Nonconforming forms

- **9. NONCONFORMING FORMS**
- Please identify all unauthorized forms to the CMS Manager as soon as possible. Include location and a timeline for bringing the form into compliance. Any unauthorized forms found without a plan of action for conforming to this standard will be removed or quarrantined without announcement.
-

Updating your signature



E-mail account: neely.a.snyder.civ@mail.mil

New messages: Neal

Replies/forwards: ME

→Cell 210-238-5293 ←

Alt. 443-987-2153
Office: 210-466-0116
DSN 312-450-0116
"We Are the Army's Home --
Serving the Rugged Professional"
Learn more about us at https://home.army.mil/imcom

1. Click on the File tab
2. Select Options
3. Select Mail
4. Select Signatures
5. In the Select Signatures box, choose the sig
you'd like to edit.
6. Make your changes
(https://home.army.mil/imcom)
7. Click OK
8. Click OK
9. Feel OK.

"Nailed it!"

-30-

IEW SOP/Tutorials:

1.Getting Started; Adding Text, Images and Links

2.Adding and working with pages

3.Adding and working with blocks

4.Working with files

5.Accounts

6.Permissions

7.Site management operations

8.Phonebook and special features

9.Advanced site management, design and standards

10.General policies

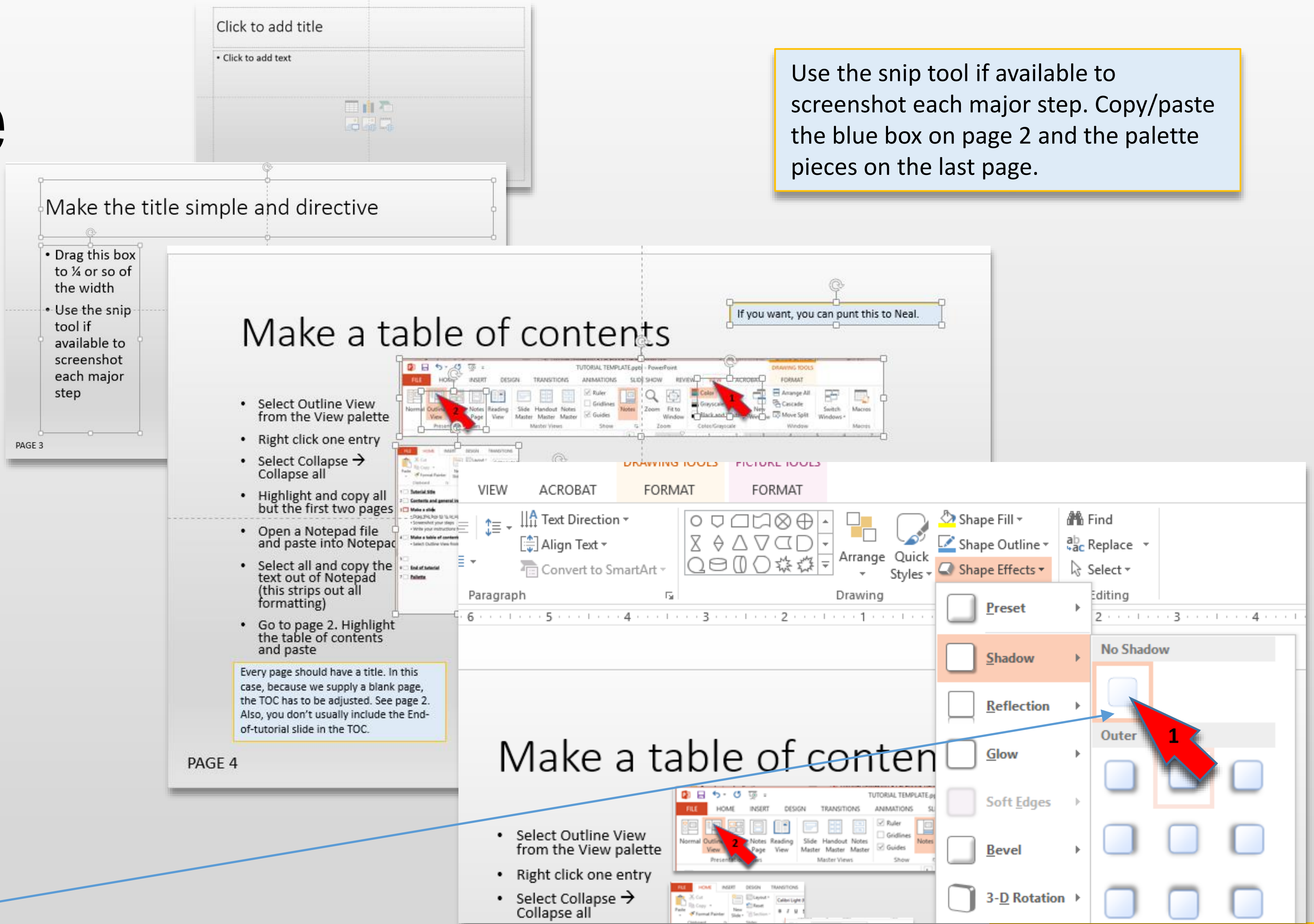
End of tutorial

Backup material follows

Make a slide

- Drag this box to ¼ or so of the width
- Screenshot your steps. Cut/paste the arrows from the palette page
- Write your instructions here
- Highlight all of your graphic elements and apply a shadow to make them distinct from one another

Use the snip tool if available to screenshot each major step. Copy/paste the blue box on page 2 and the palette pieces on the last page.



Click to add title

- Click to add text

Make the title simple and directive

- Drag this box to ¼ or so of the width
- Use the snip tool if available to screenshot each major step

PAGE 3

Make a table of contents

If you want, you can punt this to Neal.

- Select Outline View from the View palette
- Right click one entry
- Select Collapse → Collapse all
- Highlight and copy all but the first two pages
- Open a Notepad file and paste into Notepad
- Select all and copy the text out of Notepad (this strips out all formatting)
- Go to page 2. Highlight the table of contents and paste

Every page should have a title. In this case, because we supply a blank page, the TOC has to be adjusted. See page 2. Also, you don't usually include the End-of-tutorial slide in the TOC.

PAGE 4

Make a table of conten

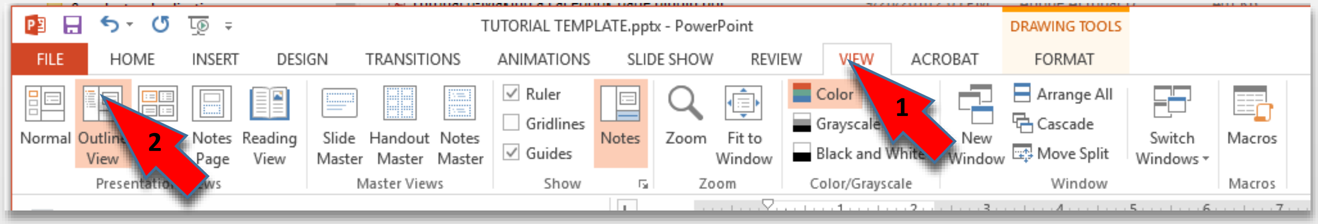
- Select Outline View from the View palette
- Right click one entry
- Select Collapse → Collapse all

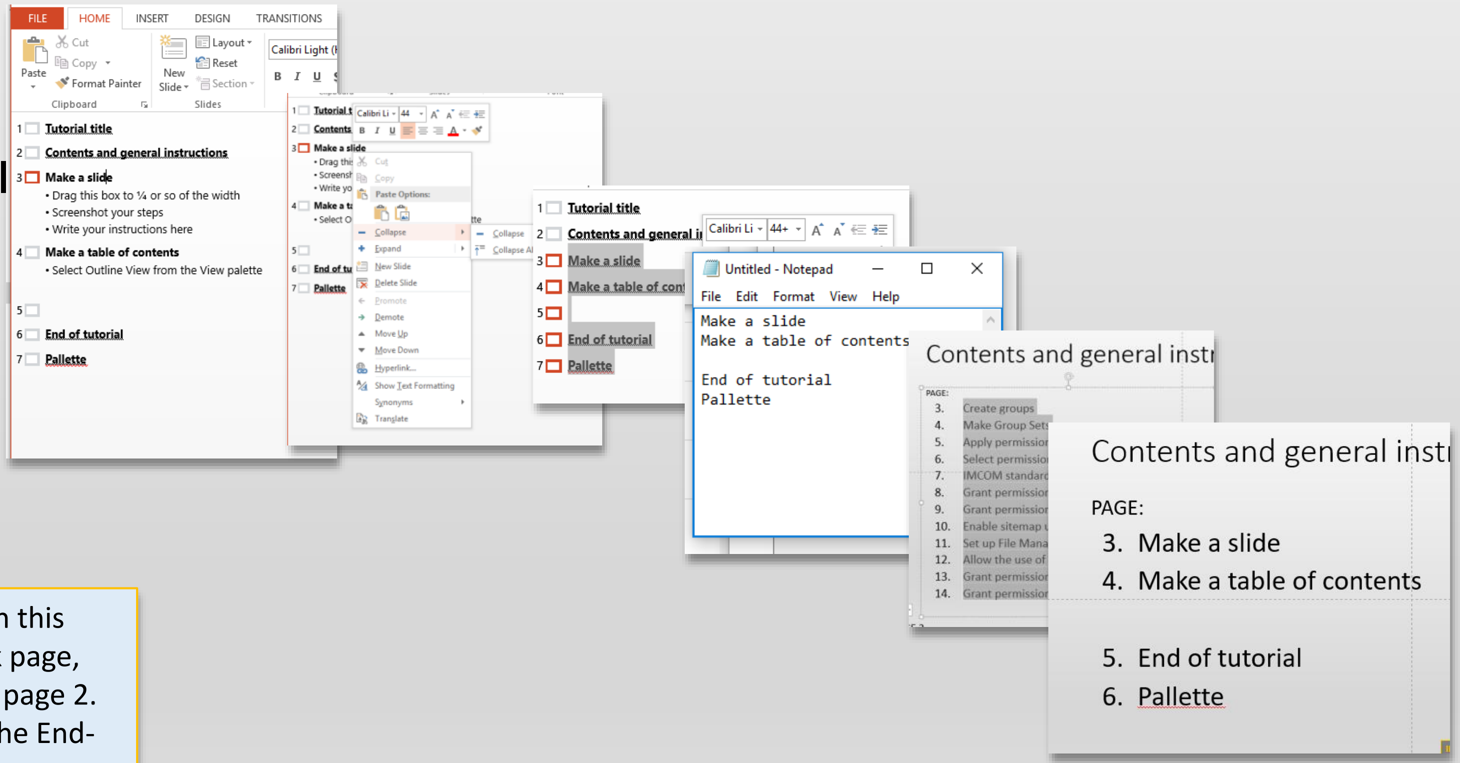
Blue boxes offer helpful explanations

Make a table of contents

If you want, you can punt this to Neal.

- Select Outline View from the View palette
- Right click one entry
- Select Collapse → Collapse all
- Highlight and copy all but the first two pages
- Open a Notepad file and paste into Notepad
- Select all and copy the text out of Notepad (this strips out all formatting)





1 Tutorial title
2 Contents and general instructions
3 Make a slide
- Drag this box to ¼ or so of the width
- Screenshot your steps
- Write your instructions here

4 Make a table of contents
- Select Outline View from the View palette

5
6 End of tutorial
7 Pallette

```
Make a slide
Make a table of contents

End of tutorial
Pallette
```

Contents and general instr

PAGE:
3. Create groups
4. Make Group Sets
5. Apply permission
6. Select permission
7. IMCOM standard
8. Grant permission
9. Grant permission
10. Enable sitemap
11. Set up File Mana
12. Allow the use of
13. Grant permission
14. Grant permission

Contents and general inst

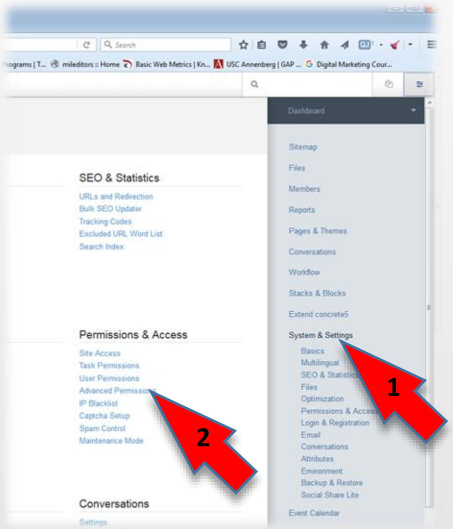
PAGE:
3. Make a slide
4. Make a table of contents

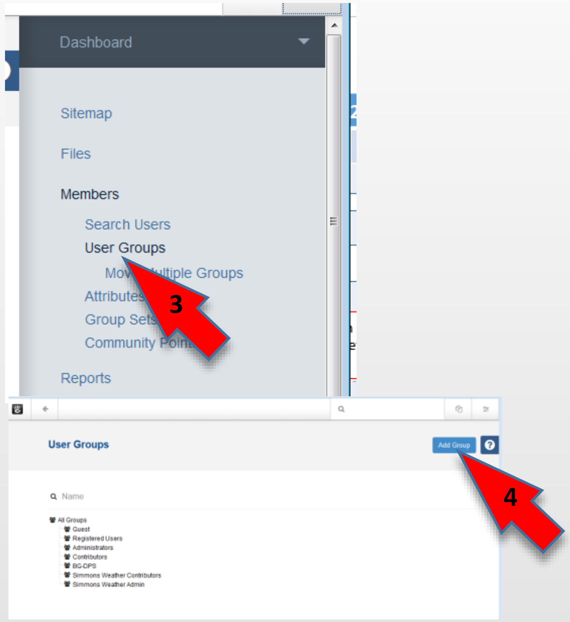
5. End of tutorial
6. Pallette

Every page should have a title. In this case, because we supply a blank page, the TOC has to be adjusted. See page 2. Also, you don’t usually include the End-of-tutorial slide in the TOC.

Palette

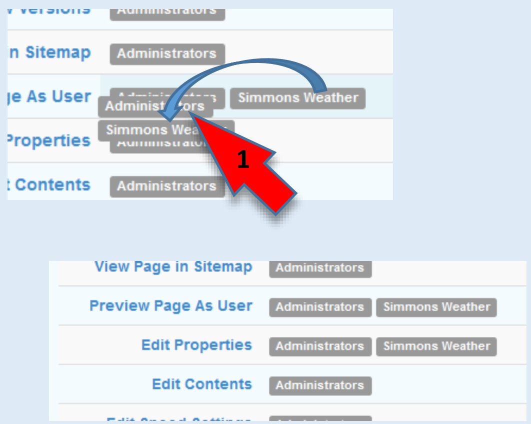
- Copy and paste these arrows and boxes.





Drag and Drop

....to duplicate permissions from one action to another!



NAMING CONVENTION:

"UID last 2-Group name-Admin or Contributors"

BG-Simmons Weather Contributors

BG-Simmons Weather Admin

Start with the last two letters of your garrison unit ID (eg. Fort Bragg is "BG") "Contributors" groups should not have publication permission. Use "Admin" for those who have publishing rights to a page.

Use the same name for the page, groups and sets.

UID=Unit ID. For IMCOM garrisons, it's four characters starting with IM – for Fort Bragg, it's IMBG. Thus, BG is the Fort Bragg prefix.

A CERTIFIED AGENT is a person allowed by PAO to post to a section of a website. They must have certifications specified in the IMCOM Enterprise Web SOP and operate under garrison PAO oversight.