DEPARTMENT OF THE NAVY
COMMANDER NAVY RESERVE FORCE
1915 FORRESTAL DRIVE
NORFOLK, VIRGINIA 23551-4615

COMNAVRESFORINST 5239.3B
N64
1 Sep 24

COMNAVRESFOR INSTRUCTION 5239.3B

From: Commander, Navy Reserve Force

Subj: NAVY RESERVE FORCE INFORMATION ASSURANCE AND PERSONALLY IDENTIFIABLE INFORMATION PRIVACY PROGRAM

Ref: (a) DoD O-8530.1-M, Computer Network Defense Service Provider Certification and Accreditation Program, December 2003
(b) DoD Directive 8570.01 of 15 August 2004
(c) COMNAVRESFORINST 5239.4 (Series)
(d) DoD Directive 8500.01E of 24 October 2002
(e) SECNAVINST 5239.3B
(f) OPNAV 5239/14 (Rev. 9/2011)
(g) DOD Instruction 8500.01 (Series)
(h) DOD Instruction 8510.01 (Series)
(j) SECNAVINST 5211.5 Series
(k) DON memo of 3 Jul 07
(l) DON CIO 181430Z May 09
(m) NIST Special Publication 800-34 of May 10
(n) DoD Instruction 8500.2 of 6 February 2003
(o) OPNAVINST 5239.1C
(p) ALNAV 001/16 DON Electronic Spillage Reporting Process
(q) COMNAVNETWARCOM 021854Z May 11
(r) DON CIO 171952Z Apr 07
(s) DON CIO 081745Z Nov 12
(t) SECNAV 042232Z Oct 07
(u) Office of the Undersecretary of Defense memo of 7 Jun 13
(v) SECNAVINST 5520.3B
(w) DoD 5200.2-R, Personnel Security Program, January 1987
(x) DON CIO 291600Z Feb 08

Encl: (1) Definition of Terms
(2) Minimum Program Requirements
(3) Revised DON Guidance for Marking Documents Containing (PII)

1. Purpose. The purpose of the Commander, Navy Reserve Force (COMNAVRESFOR) Information Assurance (IA) and Personally Identifiable Information (PII) privacy program is to ensure COMNAVRESFOR Information Technology (IT) resources can be employed in a way that allows mission owners and operators to have confidence in the confidentiality, integrity and availability of those resources and the information they contain and transmit and to make choices based on that confidence per references (a) through (aa) and enclosure (1) and (2). This instruction is a complete revision and should be reviewed in its entirety.

a. Additionally, this instruction will:

(1) Define the organizational structure of COMNAVRESFOR IA, PII and Cybersecurity Workforce (CSWF) programs.

(2) Apply basic policy and principles of security as they relate to IT and Information Systems (IS) associated with networks, web sites and applications used or owned by the Navy Reserve including Navy Marine Corps Internet (NMCI) and the Navy Reserve Homeport.

2. Cancellation. COMNAVRESFORINST 5239.3A.

3. Definitions. Enclosure (1) defines relevant terms.

4. Objective. Per references (n) and (s), the COMNAVRESFOR IA and PII policy shall, consistent with Federal Information Security Management Act (FISMA), Department of Defense (DoD) and Department of the Navy (DON) policies and guidance:

a. Provide guidance for implementation of IA protections commensurate with the risk and magnitude of the harm resulting from unauthorized access to, use, disclosure, disruption, modification or destruction of:

(1) Information collected or maintained by or on behalf of COMNAVRESFOR.

(2) IS used or operated by COMNAVRESFOR, by a COMNAVRESFOR contractor processing Navy information or by other organizations on behalf of COMNAVRESFOR.

b. Establish a methodology to protect the availability, integrity, authentication, confidentiality and non-repudiation of IS.

c. Identify, train and certify personnel performing IA functions as part of CSWF, which includes military, Government employees and contractor personnel per references (a) through (c) and (x).

d. Ensure all authorized users of COMNAVRESFOR IS and the NMCI complete the current IA awareness training course, PII training course and thereafter complete annual IA and PII refresher trainings as required by references (d) through (f).

e. Require COMNAVRESFOR IS that meet the qualification for registration in DoD IT Portfolio Repository (DITPR) to be registered.

f. Require that all IS under COMNAVRESFOR authority that require Assessment and Authorization (A&A) are accredited per references (g) and (h).

g. Evaluate COMNAVRESFOR IA policies and procedures annually.

h. Ensure compliance with DoD IA Vulnerability Assessment notification and corrective action process.

i. Ensure COMNAVRESFOR compliance with Federal regulations and laws pertaining to the protection of PII within IS per references (j) through (l).

5. Scope. This instruction applies to IS and networks operated by COMNAVRESFOR activities that enter, process, store or transmit unclassified, sensitive or classified information. This instruction and all applicable references apply to all military, government and contractor personnel within the COMNAVRESFOR claimancy. It encompasses all IS and networks that are procured, developed, modified, operated, maintained or managed for COMNAVRESFOR.

6. Authority. Ultimate responsibility for acceptance of the risk inherent in all COMNAVRESFOR IS rests with the Navy Authorizing Official (NAO). Navy Network Warfare Command (NNWC) maintains NAO for all DON IS. COMNAVRESFOR Echelon II (ISSM) coordinates with the NAO for all applicable IS.

7. Precedence. Policy and requirements set forth by higher authority take precedence over the policy established in this instruction, except where this instruction is more restrictive. Implementing authorities should identify conflicting policy to the COMNAVRESFOR ISSM (N64) for resolution.

8. Policy

a. General. All COMNAVRESFOR activities shall maintain an aggressive IA program that appropriately safeguards information, resources and PII at all times with respect to confidentiality, integrity, availability, authentication and non-repudiation. Safeguarding IT resources and information shall be accomplished through the employment of defensive layers that include the IA disciplines, as well as sound administrative practices that include budgeting, funding and executing the actions necessary to protect all IS resources.

b. Local IA Authority. Commanders, Commanding Officers (CO) and Officers in Charge (OIC) are designated as the Local IA Authority for their command. This authority and responsibility shall not be delegated. The COMNAVRESFOR Chief Information Officer (CIO) is designated as the Local IA Authority for the Reserve Component (RC). The CIO is represented by a Force ISSM, N64, operating at Commander, Navy Reserve Forces Command. The Force ISSM acts as the central information authority for all Reserve Force IA matters.

c. IA Personnel, Training, Certification and Management

(1) All RC personnel, government and contractor, performing IA functions must be properly trained and certified as part of the CSWF as required by references (a) through (c).

(2) All RC personnel performing IA functions shall be identified, tracked and monitored to ensure that IA positions are staffed with trained and certified personnel. All RC activities shall establish, resource and implement an IA/Cybersecurity training and certification program for all IA personnel per references (a) through (c).

(3) Statements of work, position descriptions and contracts shall identify all IA functions and requirements to be performed by contractor personnel working within RC activities.

(4) All authorized users of RC IS, including NMCI, must complete DoD IA/Cyber Awareness Training as a condition of network access. The Local IA Authority is encouraged to add to the standardized baseline training their local IA policies and procedures. DoD IA training is as follows:

(a) Initial IA awareness training, current version.

(b) Annual IA refresher awareness training.

(5) All RC personnel, government and contractor, who require privileged access to RC IS and networks within RC activities must complete a Privileged Access Agreement (PAA) per reference (c). RC activities may expand the requirements of this agreement to meet their needs.

(6) All personnel assigned to IA positions within RC activities shall be CSWF compliant at the time of their appointment/assignment or become fully compliant no later than one year from the date of their appointment/assignment. Temporary waivers to the CSWF requirement for IA professionals may be requested, but are discouraged.

d. Contingency Planning. Echelon III contingency plans (CP) shall be developed, tested and evaluated on an annual basis, to the maximum extent feasible. CP shall describe the interim measures used to recover and restore IT systems and service operations following an emergency or system disruption. The CP must provide specific guidance and be incorporated into the site's Continuity of Operations Plan.

(1) CP must adhere to reference (m).

(2) The system User Representative and Program Manager (PM) must approve and sign the CP.

(3) Exercises must be documented, signed and dated. Documentation must include the name of the system and must specifically state what was tested and the results. Shortfalls shall be documented and approved by a Plan of Action and Milestones (POA&M). The POA&M shall be maintained to track progress and resolution of identified shortfalls.

e. Assessment and Authorization. All RC IS shall be authorized by the NAO prior to being placed into operation.

(1) Assessment is the comprehensive evaluation of the technical and non-technical security features of IS and other safeguards to establish the extent that a particular design and implementation meets a set of specified security requirements. The assessment process results in a risk based determination for operational use and authorization recommendation to the NAO.

(2) Authorization is the formal declaration by the NAO that an IS is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk.

(3) Full authorization with an Authority to Operate (ATO) is always the goal for operational systems.

(4) Program Managers of IS will prepare and submit type authorization to COMNAVRESFOR (N64) Cybersecurity Division, who will review and forward to the NAO. COMNAVRESFOR (N64) will coordinate with all agencies in efforts to gain system ATOs.

f. User Access. IT, network or other computer resources will follow the least privilege principle so that each user is granted access to only the information to which the user is authorized. This is done based on individual's security clearance and formal access approval to resources necessary to perform assigned functions. In the absence of a specific positive access grant, user access shall

default to no access. User's ability to access network resources will depend on completion of annual IA security training. A user's delinquency in completing this training without justification may result in Force ISSM disabling that user's account. Users with network access must comply with all provisions of enclosure (e) and the System Access Agreement Request Navy (SAAR-N) must be completed entirely, meeting these requirements:

(1) Commands must ensure Parts I, II (except item 17) and III are filled out entirely. For blocks 15-16, a Supervisor is defined as an E7 or above for military or a GS-12 or above for civilians. The Security Manager (SM) must verify status in Part III with the following conditions:

(a) If a required investigation does not exist for an individual, the proper paperwork shall be submitted and accepted prior to granting network access.

(b) If an investigation requires periodic reinvestigation and the proper paperwork is not submitted and accepted within six months, the CO shall restrict network access.

(c) If an individual has an adjudicative determination of "Revoked" or "Denied," the CO and Security Manager (SM) shall review the circumstances to determine whether network access should or should not be restricted. If unable to resolve after one year, the CO shall coordinate with the Readiness and Mobilization Command ISSM to restrict network access.

(d) If any paperwork is submitted and accepted for initiation and/or adjudication of a background investigation, the CO and SM shall review the package in its entirety before granting or continuing network access.

(e)Users must login to the profile specific to their role. For example, a Navy civilian who is also a SELRES must login to their civilian account when performing civilian duties and their SELRES account when performing SELRES duties.

g. Electronic Spillages. An electronic spillage is defined as data placed on an IT system possessing insufficient security controls to protect the data at the required classification level (i.e., secret data onto unclassified).

(1) RC commands that originate an electronic spillage shall follow the requirements of reference (p):

(a) Report the spillage to their Command Security Manager (CSM) to ensure proper handling and reporting of all potential compromises of classified information. This will include actions to initiate a Preliminary Inquiry and coordination with the Original Classification Authority for a classification determination to verify whether or not an electronic spillage occurred. CSM must immediately report and forward all information to the Echelon II SM.

(b) Coordinate with the COMNAVRESFOR ISSM to preclude further dissemination of the spillage, report the spillage as required by established Navy electronic spillage policy annotated in reference (p) and initiate spillage clean-up actions as appropriate.

(c) In the course of completing a private investigation, gather as much information as possible regarding the incident, including affected users and assets. Secure hardware as appropriate

to prevent further dissemination of the spillage.

h. Use of Removable Storage Media. This policy applies to any removable storage media that may be connected to a Navy network, workstation or other computing device via cable, Universal Serial Bus (USB), infrared, radio frequency, or any other external connection that would allow data to be transferred and removed. Examples of removable storage media include, but are not limited to recordable and re-writable Compact Disks (CD), recordable and re-writable Digital Video Disks (DVD) and mini external hard drives.

(1) Removable storage media on classified computing devices:

(a) Due to inherent risks associated with removable storage media, restrict access to use of all USB ports.

(b) Connecting any removable storage media to a classified IT system or network will make the storage device permanently classified at the same level as the system.

(2) General use:

(a) Use of removable storage media on Navy networks will be limited to those who have an operational necessity to use the device. Where this requirement applies, commands will use government furnished storage devices on the NMCI Certified Device List (CDL) available on the NMCI Homeport website at: https://www.homeport.navy.mil/home/. These devices provide the capability to encrypt data stored on them using commercially available encryption technology. Only DON approved enterprise Data at Rest (DAR) products may be used.

(b) Connecting personally owned removable storage media, including personal devices, to a Navy network is prohibited. Violation of this policy will result in denial of a user's network access. When this occurs, personnel must be counseled by an Echelon IV (or higher) ISSM, repeat the current version of annual IA awareness training and submit another SAAR form before access is restored.

(c) Any removable storage media affected by an electronic spillage will be surrendered to the command ISSM or Information Systems Security Officer (ISSO) immediately until properly sanitized. Media that cannot be sanitized will be rendered unusable and destroyed per reference q).

(d) All removable storage media will be labeled with the highest overall classification level using the appropriate label (Standard Form 706, 707, 708, 709, 710) and include the abbreviated form of all applicable warning notices. If forms are not available, mark all removable storage media with a permanent marker. This requirement includes markings of "unclassified" CDs and DVDs.

(e) Immediately report to the CSM if any removable storage media containing classified or Controlled Unclassified Information (including PII is lost or stolen).

(f) All unclassified DoD data at rest stored on removable storage media shall be treated as sensitive data and encrypted using commercially available encryption technology. Only DON approved enterprise DAR products may be used.

(g) Digital cameras purchased by COMNAVRESFOR, used by the command in an official capacity, issued to a responsible party and secured after use are authorized to connect to the network for the purpose of downloading photographs. Commands must submit a memorandum of compliance listing camera make/model to the Echelon IV, III or II ISSM, as applicable, for the record.

i. Protection of Sensitive Information. All unclassified DoD DAR that has not been approved for public release shall be treated as sensitive data. COs and OICs of RC commands shall ensure sensitive information is protected per references (a) through (d) and (f).

(1) DoD sensitive data shall remain on the DoD network. Auto-forwarding DoD emails to commercial email accounts or using personal commercial email accounts to conduct Navy business is strictly prohibited.

(2) Documents and files containing DoD sensitive data shall not be transmitted to commercial email accounts or saved to personal devices.

(a) Users shall utilize the Navy Reserve Homeport (NRH) Private Portal at https://private.navyreserve.navy.mil for document sharing and collaboration. Local SharePoint Administrators and Site Owners will ensure access to NRH folders corresponds with the level of sensitive data contained. For example, if documents contain PII, they must be contained in an established folder that can be viewed and accessed only by those personnel with a specific need or valid reason to view the files.

(b) Commercial file sharing and storage sites are not approved for use by the DoD, nor are they certified and accredited by the NAO. Use of commercial file sharing sites such as www.dropbox.com is not authorized.

(c) Files may be securely transmitted using Department of Defense (DoD) Secure Access File Exchange (SAFE) web application, which supports files sizes up to 2 GB. RC users should choose the Command Access Card (CAC) options for file transmission. DOD SAFE is available at https://safe.apps.mil/and is the preferred means to safely transfer files to domains other than ".mil" addresses.

(3) Protection of PII. Commanders, COs, OICs of RC commands shall comply with privacy and security requirements of references (n), (p) and (r) through (u). PII is any information that can be used to distinguish or trace an individual's identity. Examples include but are not limited to name, social security number, date of birth, home address, home phone number, personal email address, financial information, fingerprints, photograph and medical information. The leading cause of a PII breach is human error. It is important to check all attachments for PII, particularly in Microsoft Excel spreadsheets that contain multiple tabs, particularly if columns are hidden. As such, RC commands shall:

(a) Comply with current DON/CIO guidance on CUI markings per DON/CIO guidance and enclosure (3).

(b) Ensure storage of any form of PII is not conducted on personally owned computers (to include laptops), mobile computing devices and removable storage media. The exception to this are command recall rosters, where personnel have given consent to publish personal information for

official, command recall use and where distribution is limited to command members. If command recall rosters are posted on NRH private portal, the site administrator shall ensure access is restricted to command members.

(c) The use of fax machines to send information containing PII is prohibited except for cases annotated in reference (u) where:

1. Another more secure means of transmitting PII is not available.

2. A process outside of DON control requires faxing to an activity (such as Defense Finance and Accounting Services, TRICARE, etc.).

3. Operational necessity requires expeditious handling.

4. When faxing PII related to internal government operations only (i.e., office phone number, rank, job title).

(d) Ensure any known or suspected breach of PII is reported immediately to the regional PII Officer and COMNAVRESFOR N64 Reserve Force ISSM. Reporting procedures will be the responsibility of the local command responsible for the breach and must be per the procedure outlined in reference (v). All Breaches are now reported through the Department of Defense (DoD) Privacy/Freedom of Information Act (FOIA) Information Management System (DPIMS) website, https://dpims.disa.mil/eCase/Home2.aspx.

(e) Ensure Privacy Impact Assessment (PIA) is completed for all IS requiring a PIA per reference (w).

(f) A PII spot check shall be performed on a quarterly basis. The results of the spot check shall be maintained as an auditable item for 3 years after completion per reference (aa). Several examples of PII spot check forms can be found at http://wwww.doncio.navy.mil. The spot check form should be tailored for the specific needs and use of the command. These spot checks shall include any web or SharePoint pages the command uses or is responsible for maintaining.

(g) COMNAVRESFOR (N6) will perform a quarterly search of all files on the NRH. Any unprotected file found to contain PII will be moved to a secure location and the command will be notified. Upon notification, the command is required to report the breach to the DON CIO Privacy Office per reference (v) and perform all actions as directed by the Privacy Office.

(h) Per reference (u), ECH IV Commands manages and distributes all mobile computing devices (laptops, smart phones, tablets, etc.) as need. ECH IV and ECH V Commands uses DD Form 2501 to ensure all computing devices are issued properly. Commands will verify custody of these devices annually.

(i) Each command shall conduct a semi-annual review of all paper records containing PII to ensure their destruction when retention is no longer required.

(j) Each command shall conduct a semi-annual review of all electronic files, including but not limited to share drives, SharePoint, command websites and email, containing PII to ensure destruction when retention is no longer required.

(k) Each command shall conduct an annual review of all locally generated documents for PII requests and determine if the requirement to collect the information still exists or if the form may be altered.

(4) Unless listed on the NMCI CDL, Bluetooth devices are not authorized for use on government networks.

j. Annual Reviews and Tests. All IS must undergo annual information security reviews per references (h) and (k). Corrective action shall be taken to address shortfalls identified. If an ATO is awarded during the year, this suffices for the annual review. However, in succeeding years, systems must be reviewed for any changes that could affect the accreditation. Completion of the review must be noted in the FISMA section of the DITPR-DON and fall within 12 months of the previous completion date.

k. IA Vulnerability Management. The IA Vulnerability Management (IAVM) process is designed to provide positive control of the vulnerability notification and corrective action process in DoD. Commanders/COs of RC activities shall comply with the IAVM process and report Information Assurance Vulnerability compliance as required.

l. Digital Signature. Email messages requiring either message integrity or non-repudiation must be digitally signed using DoD Public Key Infrastructure (PKI) per reference (p). This includes emails that direct/task or pass direction/tasking, requests or responds to requests for resources, discusses any operational matter, discusses contract information, financial or funding matters, personnel management matters, where the need exists to ensure that the email originator is the actual originator and where the need exists to ensure that the email content has not been tampered with while in transit. All email containing an attachment or embedded active content (e.g. Hyperlink to a uniform resource locator or active code) must also be digitally signed.

m. Encryption. All sensitive information, to include PII (excluding work signature block with rank, work email address and phone number) and controlled unclassified information contained in either email or web server transactions is to be encrypted using DoD PKI. This provision also applies to any email that discusses any matter that may serve as an operations security indicator.

(1) Personnel are only able to transmit an encrypted email if the recipient has published their public certificate to the Global Access List (GAL) within NMCI. As an alternative, encrypted emails can be sent by receiving a digitally signed email from a user, then adding that user to your contact list. If an email recipient cannot receive an encrypted email, notify them in a separate email. In these cases, do not send sensitive information unencrypted.

n. Use of IT Assets While on Travel

(1) All RC personnel have the inherent responsibility to continually promote safe, effective and legal use of all IT resources. RC government and contractor personnel must:

(a) Exercise the highest standards of professionalism and responsible behavior with the information they obtain from or make available on the Internet and during email communications and act to protect the interests of national security.

(b) Minimize the risk of unauthorized access by traveling with only the minimum required computer assets and data.

(c) Keep in mind there is no assurance of privacy in their use of a computer system/laptop when connected to the Internet, especially overseas and when connected to the Internet and using email, this connection is subject to monitoring, interception, accessing and recording.

(d) Notify your chain of command, the site Security Office and Naval Criminal Investigative Service as soon as possible in the event of any loss of control over or compromise of IT assets or suspicious activity.

(2) RC personnel traveling overseas/Outside the Continental United States (OCONUS) shall:

(a) Immediately report to the command ISSM the loss of control for any period of time, a DoD IT asset, whether by loss, theft, confiscation, temporary misplacement or the like.

(b) Consult and notify the command ISSM whenever necessary to obtain proper guidance for computer security issues.

(3) When overseas/OCONUS on official government travel, RC government or contractor personnel may not:

(a) Use a non-DoD computer for official business or OWA unless specifically approved by the Local IA Authority.

(b) Store and/or transport government data on personally owned or foreign-supplied portable/removable devices.

(c) Use or access personal email accounts for official government business.

o. Classified Information on the Public Domain

(1) Per reference (x) COMNAVRESFOR military, government and contractor employees shall not access or download documents that are known or suspected to contain classified information on the unclassified internet. This applies to both government and personal devices that access the DoD Information Network remotely including via OWA or other remote access.

(2) Personnel who inadvertently discover potentially classified information on the public domain shall immediately report it to their SM or ISSM/ISSO.

9. Responsibilities

a. COMNAVRESFOR ISSM shall:

(1) Serve as the focal point and principal advisor for IA/Cybersecurity matters for COMNAVRESFOR and the Reserve Force CIO. The Force ISSM will have a direct reporting relationship with the CIO in all matters related to the command's IA/Cybersecurity program.

(2) Liaise with the NAO for the accreditation and certification of all COMNAVRESFOR IS. The NAO is the official with authority to accredit or grant an ATO for all ISs that fall under his/her cognizance.

(3) Provide policy, coordination and management oversight of the overall COMNAVRESFOR IA program including unclassified data, program development, implementation, control, planning, programming and budgeting consistent with national goals and policies established by the DoD and DON.

(4) Ensure contract specifications for IS equipment, software, maintenance and professional services satisfy IA requirements.

(5) Ensure security requirements are included in life cycle management documentation. Security will be built into systems, whenever possible, to prohibit users from accessing restricted and/or need-to-know only information.

(6) Monitor Naval telecommunications directives and communication tasking orders released by United States Cyber Command and implement all requirements.

(7) Maintain professional certifications as a member of the CSWF. Provide policy and direction to RC on all CSWF requirements.

(8) Be designated in writing as Force ISSM by the Commander.

(9) Ensure that all users have the requisite security clearances and access authorization and are aware of their Cybersecurity responsibilities before being granted access to DoD IS and platform IT systems.

(10) Issue guidance and deadlines for the completion of annual IA/Cyber Awareness and PII Training that meet DoD and DON guidelines each fiscal year. Direct account disablement action for COMNAVRESFOR users delinquent in either training.

b. Echelon IV ISSMs shall:

(1) Ensure the development of a regional IA program to provide adequate security to protect all IS, properly train all personnel, implement security plans, procedures, risk assessments, contingency plans and ensure compliance with all DoD, DON and RC directives.

(2) Provide policy, coordination and management oversight of the overall COMNAVRESFOR IA/Cybersecurity program including unclassified data, program development, implementation, control, planning, programming and budgeting consistent with national goals and policies established by the DoD and DON.

(3) Be designated in writing by the Readiness and Mobilization Command Commander as Regional ISSM.

(4) Ensure that all users have the requisite security clearances and access authorization and are aware of their Cybersecurity responsibilities before being granted access to DoD IS and platform IT systems.

(5) Enforce annual IA/Cyber Awareness Training requirement and follow direction of higher echelon.

c. Echelon V ISSO shall:

(1) Enforce all security requirements implemented by the ISSM.

(2) Ensure all countermeasures required to protect data, devices and information are in place.

(3) Provide support and report to the ISSM on all IA matters.

(4) Report security violations/incidents, as appropriate.

(5) Develop and manage a program to implement DoD, DON, Chief of Naval Operations and COMNAVRESFOR IA policy.

(6) Provide support to COMNAVRESFOR teams performing computer security inspections and audits, as requested.

(7) Provide security training expertise or assistance, as necessary and conduct annual IA and PII training.

(8) Ensure that all users have the requisite security clearances and access authorization and are aware of their Cybersecurity responsibilities before being granted access to DoD IS and platform IT systems.

d. PMs shall:

(1) Exercise the appropriate life cycle management practices to ensure their programs receive the proper IA certification and accreditation before being placed into operation. Ensure ATO status is maintained through annual review of system package or when changes occur that affect the security posture of the system.

(2) Ensure Navy information entered, processed, stored or transmitted by IS is adequately protected with respect to confidentiality, integrity, availability and privacy per this instruction and application DoD and DON policies.

(3) Ensure all personnel supporting IS with privileged access are qualified as required as part of the CSWF and have a signed PAA.

e. COs/OIC, of RC commands shall:

(1) Act as the Local IA Authority for their command. The responsibility of the Local IA Authority may not be further delegated.

(2) Appoint in writing, an ISSM for Echelon IV commands and an ISSO for Echelon V commands.

(3) Establish and implement security mechanisms and procedures to ensure that information

entered, processed, stored or transmitted by COMNAVRESFOR IS is adequately protected with respect to confidentiality, integrity, availability and privacy.

(4) Ensure physical security measures are appropriate to protect COMNAVRESFOR information and resources.

(5) Implement procedures for reporting identified and/or suspected IS security violations.

(6) Develop and implement local policy and procedures to support effective employment of anti-virus software on the personal devices of Selected Reserve Sailors and Full Time Support staff. The DoD licensed anti-virus software should be used where feasible, available at www.disa.mil.

(7) Implement policy whereby information on the NRH is reviewed and approved by appropriate authorities prior to posting to ensure that all information will be protected commensurate with the sensitivity level of the information. Public facing web sites outside of the COMNAVRESFOR-hosted domain (www.navyreserve.navy.mil) are not authorized.

(8) Ensure initial Cyber Awareness/IA training is provided for all new personnel. Training shall be conducted prior to issuance of networks and IS access authorization. Ensure annual Cyber Awareness/IA training is completed for all personnel.

(9) Ensure all personnel performing IA functions are identified and tracked as members of the CSWF and monitored to ensure they are properly trained and certified.

f. Privileged User with Cybersecurity responsibilities (e.g. System Administrator). Privileged users, in addition to satisfying all responsibilities of an Authorized User, shall configure and operate IS within authorities vested in them
according to DoD Cybersecurity policies, procedures and notify the ISSM of any changes that might impact security posture.

g. Authorized User. Each Authorized User shall:

(1) Immediately report Cybersecurity events, potential threats and vulnerabilities to the appropriate ISSM or ISSO.

(2) Protect terminals, workstations or other output devices and resident data from unauthorized access.

(3) Inform the ISSM or ISSO when access to a particular DoD IS or platform IT system is no longer required (e.g., completion of project, transfer, retirement, resignation).

(4) Observe policies and procedures governing the secure operation and authorized use of DoD IT.

(5) Use DoD IT only for authorized purposes.

(6) Not unilaterally bypass, strain or test Cybersecurity mechanisms.
(7) Not introduce or use unauthorized software, firmware or hardware on DON IT.

(8) Not relocate or change IT equipment or the network connectivity of equipment without proper authorization.

(9) Protect CAC and Secret Internet Protocol Router Network (SIPRNet) token (if applicable) to the maximum extent possible.

10. Action. COMNAVRESFOR commands will implement this guidance within their command.

11. Records Management. Records created as a result of this instruction, regardless of media and format, must be managed per Secretary of the Navy (SECNAV) Manual 5210.1 of January 2012.

12. Review and Effective Date. Per OPNAVINST 5215.17A, COMNAVRESFORCOM will review this instruction annually on the anniversary of its effective date to ensure applicability, currency, and consistency with Federal, DoD, SECNAV, and Navy policy and statutory authority using OPNAV 5215/40 Review of Instruction. This instruction will automatically expire 5 years after effective date unless reissued or canceled prior to the 5-year anniversary date, or an extension has been granted.

M. J. STEFFEN
Deputy Commander

Release and distribution:
This instruction is cleared for public release and is available electronically only via Commander, Navy Reserve Force Website, https://www.navyreserve.navy.mil/Resources/Official-Guidance/Instructions/.

Definition of Terms

1. Authorization. A formal declaration by the NAO that an IS, network or computer resource is approved to operate in a particular security mode using a prescribed set of safeguards. Accreditation is the official management authorization for operation and is based on the certification process as well as other management considerations. The accreditation statement affixes security responsibility with the NAO and shows that due care has been taken for security.

2. Asset. Any software, data or hardware resource within an IS or network.

3. Assessment. The technical evaluation made as part of and in support of the authorization process, that establishes the extent to which a particular computer system or network design and implementation meets a prespecified set of security requirements.

4. Contingency plan. A plan for emergency response, backup operations and post disaster recovery maintained by an activity as a part of its information security program. The plan is a comprehensive statement of all the planned actions to be taken before, during and after a disaster or emergency condition. This statement shall include documented, tested procedures to ensure the availability of critical computer resources and facilitate maintaining the continuity of IS operations in an emergency situation.

5. Data integrity. The state that exists when data is unchanged from its source and has not been subjected to accidental or malicious modification, unauthorized disclosure or destruction.

6. Denial of service. Action or actions that result in the inability of an IS or any essential part to perform its designated mission, either by loss or degradation of operational capability.

7. NAO. Official with the authority to formally assume responsibility for operating an IS or network at an acceptable level of risk.

8. DoD Risk Management Framework (RMF). The standard DoD approach for identifying information security requirements, providing security solutions and managing IS security activities.

9. IA. Information operations that protect and defend information and IS by ensuring their availability, integrity, authentication, confidentiality and nonrepudiation. This includes providing for restoration of IS by incorporating protection, detection and reaction capabilities.

10. IS. An assembly of computer hardware, software and/or firmware configured to collect, create, communicate, compute, disseminate, process, store and/or control data or information.

11. IS Security. Measures to protect against unauthorized (accidental or intentional) disclosure, modification or destruction of IS, networks and computer resources or denial of service to process data. It includes consideration of all hardware and software functions, characteristics and/or features operational procedures, accountability procedures and access controls at the central computer facility, remote computer and terminal facilities; management constraints; physical structures and devices and personnel and communication controls needed to provide an acceptable level of risk for the IS or network and data contained therein.

12. ISSM. The person responsible to the NAO to ensure that an COMNAVRESFOR (IS) is approved, operated and maintained under the conditions of the ATO documents.

13. ISSO. The person responsible to the ISSM for the day-to-day operation and security of an IS or network.

14. Need-to-know. A determination made in the interest of U.S. national security by the custodian of classified or sensitive unclassified information, that a prospective recipient has a requirement for access to, knowledge of or possession of the information to perform official tasks or services.

15. Network. The interconnection of two or more independent IS components that provides for the transfer or sharing of computer system assets. It is composed of a communications medium and all components attached to that medium whose responsibility is the transfer of information. Such components may include IS packet switches, telecommunications controllers, key distribution centers and technical control devices.

16. PII Definition. Information about an individual that identifies, links, relates or is unique to or describes him or her, e.g., a social security number (including last four), age, rank, grade, marital status, race, salary, home/office phone numbers, demographic, biometric, personnel, medical and financial information.

17. Risk. A combination of the likelihood a threat shall occur, the likelihood a threat occurrence shall result in an adverse impact and the severity of the resulting adverse impact.

18. Risk assessment. An analysis of computer system and network assets, vulnerabilities and threats to determine the security requirements which must be satisfied to ensure the system can be operated at an acceptable level of risk.

19. Risk management. A process through which undesirable events can be identified, measured, controlled and prevented so as to effectively minimize their impact or frequency of occurrence. The fundamental element of risk management is the identification of the security posture, i.e., the characteristics of the functional environment from a security perspective. Risk management identifies impact of events on the security posture and determines whether or not such impact is acceptable and, if not acceptable, provides for corrective action. Risk assessment, Security Test and Evaluation and contingency planning are parts of the risk management process.

20. Sensitive Compartmented Information. Information and material requiring special controls for restricted handling within compartmented intelligence systems and for which compartmentation is established.

21. Sensitive UNCLASSIFIED information. Any information loss, misused, unauthorized access to or modification could adversely affect the United States national interest, the conduct of DON programs or the privacy of DON personnel (e.g., Freedom of Information Act exempt information).

22. Virus. A parasitic program that replicates itself by attaching to other programs and files intended to carry out unwanted and sometimes damaging operations. Replication usually occurs during copying of files to magnetic media or during computer-to-computer communications. The code

usually contains malicious logic that is triggered by some predetermined event. When triggered, the code then takes a hostile action against host computer systems. Additional types of computer viruses include Trojan horse, DOS, etc.

Minimum Program Requirements

1. ISSMs and ISSOs will take action necessary to ensure that these minimum requirements are satisfied in a cost-effective manner to meet the unique requirements of their area of responsibility:

a. Individual Accountability. Access to IS, network and other computer resources will be controlled and monitored to ensure each person having access can be identified and held accountable for their actions.

b. Physical Control. IS, network and other computer resources will be physically protected against damage and unauthorized access.

c. Data Integrity. Each database or collection of data elements in an IS will have an identifiable origin and use. Its use, backup, accessibility, maintenance, movement and disposition will be governed on the basis of classification, sensitivity, type of data, need-to-know and other restrictions.

d. Marking. Permanent human-readable output shall be marked to accurately reflect the sensitivity of the information. The marking may be automated (i.e., the IS has the capability to produce the markings) or may be done manually. Automated markings on output from systems which process or handle classified information must not be relied upon to be accurate unless security features and assurances of the system meet the requirements for a minimum-security class B1.

e. Access. There shall be in place an access control policy for each IS. It shall include features and/or procedures to enforce the access control policy of the information contained within the IS. The identity of each user-authorized access to IS shall be positively established before authorizing access.

f. Network/Communication Links. All communications circuits will be secured per the communications security program, reference (h). Those handling plain text classified will be installed in an approved protected distribution system. For purposes of accreditation, a network shall be treated as either an interconnection of accredited ISs (which may, themselves, be networks) or as a single distributed system.

g. Accreditation. Each IS, network or computer resource shall be accredited to operate per a NAO-approved set of security requirements.

h. Risk Management. A risk management program shall be in place to determine how much protection exists, how much
protection is required and the most economical way of providing
needed protection. Risk assessments shall be conducted:

(1) Before design approval.

(2) To support accreditation.

(3) Whenever there is a significant change to the system.

(4) At least once every 3 years.

i. Certification. Systems developers shall certify to the users and the NAO that the system's security requirements have been met and specify any constraints on the system or its environment necessary to maintain the certification.

j. Contingency Planning. Each DON activity will develop and test a contingency plan, addressing both automated and manual backup systems, to provide for continuation of its mission during abnormal operating conditions. The contingency plan will be developed, tested and maintained to ensure continued performance of mission support and mission critical functions. It must be consistent with disaster recovery and continuity of operations plans. Detail and complexity should be consistent with the value and criticality of the systems.

k. Internal Security Mechanisms. After the system becomes operational, software and files providing internal security controls, passwords or audit trails will be safeguarded at the highest level of data contained in the IS, network or computer resource. Access to internal security mechanisms will be controlled on a strict need-to-know basis.

l. Encryption. Encryption methods, standards and devices used to protect classified data processed by an IS, network or computer resource must be approved by National Security Agency.

m. Emanations Security. IS, network and computer resources shall follow the emanations security requirements of references (o) and (p).

n. Privately Owned Resources. Connection of privately owned or leased assets to any NMCI network asset is not authorized. Privately owned or leased assets shall not be used to process classified data. Privately owned or leased assets include, but are not limited to, personal computers, personal electronic devices, software, IS appliances (routers, hubs, sniffers, etc.) and Public Data Networks.

o. Data Storage. Thumb/USB drives are not permitted for data storage or transfer to NMCI assets.

p. Access Warning. A warning against unauthorized access will be displayed (physically or electronically) on all visual
display devices or other input/output devices upon initial connection, log-on or system start-up of all computer systems (direct or remote access).

q. Security Levels. All COMNAVRESFOR IS, networks or other computer resources must implement at least C2 level functionality per reference (c), provided feasible security technology is available. Hardware and software security requirements of COMNAVRESFOR computer resources should be determined per reference (c).

r. Security Training and Awareness. There shall be in place a security training and awareness program to provide training for the security needs of all persons accessing an IS, network or computer resource. The program shall ensure that all persons responsible for an IS, network, computer resource and/or the information contained therein and all persons who must access them are aware of proper operational and security-related procedures and risks. In addition, annual Cybersecurity awareness and PII training will be provided to all personnel. The program shall meet requirements of references (c) and (d). Specifically:

(1) All users are required to conduct annual IA and PII training via Navy knowledge online, Total Workforce Management System or by classroom style lecture. Completion of both training topics will be recorded in Fleet Training Management. Planning System (automatically if done online, manually if done classroom style) as directed by COMNAVRESFORCOM N64, Force ISSM.

(2) Personnel at Echelon II, III and IV levels filling key IA billets, constituting the CSWF, are required to train and earn certain commercial certifications, maintain an Individual Development Plan and stay current in certifications as required through continuing education. Specific courses, certifications and CSWF requirements are found in reference (r).

s. Operational Data. No classified or sensitive unclassified data shall be introduced into an IS, network or computer resource without first identifying its classification or sensitivity. Approval shall be obtained from the ISSM or SM where appropriate.

t. Communications Security. All COMNAVRESFOR activities will establish measures designed to deny unauthorized persons information of value that might be derived from the possession, study or interpretation of telecommunications. The measures include, but are not limited to, the following:

(1) Communication Links. Transmission and communication lines and links which provide secure communication between components of a DON IS authorized to process classified data will be secured in a manner appropriate to the highest classification of the material transmitted through such lines or links.

(2) Interface with Communications Security. A Navy Reserve activity that operates an IS requiring communication support from telecommunications networks will follow applicable Navy communications directives for the handling of classified material. The security measures will be agreed to and implemented before connecting to the communication network.

u. Removable Media. Several factors should be taken into consideration when evaluating the need for removable media. These factors include physical security, classification level and sensitivity. In environments where data loss or compromise is an issue, the use of removable, securable, data storage systems is encouraged. Fixed internal hard disks are to be avoided in systems that use classified applications and an appropriately secure space is not available.

v. Emergency Destruction. The requirement to establish a policy for the destruction of media, networks and resources in the event of an emergency shall be addressed in the overall risk management and contingency planning programs.

w. Degaussing. Commands processing classified information shall acquire and use degaussing equipment approved by the National Security Agency. COMNAVRESFORCOM N64 maintains this equipment and accepts shipments of classified hard drives for degaussing and destruction.

x. Malicious Code. Special care shall be taken to reduce the risk of introduction of malicious code, such as logic bombs, Trojan horses, trapdoors and viruses, into computer systems.

y. Public-Disclosure. Prior to public disclosure or discussion of specific IS capabilities, limitations or vulnerabilities, all members of COMNAVRESFOR shall comply with chapter 5, reference (m), DON Public Affairs Policy and Regulations.

Revised DON Guidance for
Marking Documents Containing
Personally Identifiable Information (PII)

1. Privacy information is a category of Controlled Unclassified Information (CUI). There are eight defined privacy sub-categories (listed later in this guidance). You'll notice that the terms "category" and "sub-category" are used interchangeably in the DoD and DON guidance.

This guidance provides marking instructions for the following document types that contain PII: emails, memos, spreadsheets, briefings and presentations.

This guidance does not attempt to provide marking instructions for DON forms, naval messages, or other categories of CUI. Contact those programs for guidance.

2. The procedures for marking emails and documents containing PII have changed. The privacy marking, "FOR OFFICIAL USE ONLY (FOUO) – PRIVACY SENSITIVE. Any misuse or unauthorized disclosure may result in both civil and criminal penalties" will no longer be used, and documents containing PII will be marked per the guidance below.

Many in the past added the above FOUO privacy statement or something similar to all of their emails whether or not the email contained PII by creating an email template. This should not be done. There is no equivalent CUI statement.

To be clear, the above privacy marking and "FOUO" alone are no longer valid markings and should not be used.

If a document doesn't contain CUI then it should not be marked "CUI". If the CUI marking is used, you should be able to identify the specific CUI in the document.

3. The general rule for all documents containing PII is to mark the document at the top or "banner" with "CUI" and at the bottom or "footer" with "CUI". In addition, email subject lines should also be marked "CUI".

Do not add additional descriptive wording to the "CUI" marking. For example, do not use "CUI-Privacy", "CUI-PII", or similar modifiers.

Do not go back and re-mark existing (i.e, pre-CUI program or legacy documents). If information from these "old" documents is used to create a new document, then mark the new document according to CUI program marking policy.

4. In addition to marking documents at the top and bottom with "CUI" a CUI "Designation Indicator Block" is required at the bottom of the document's first page within the "CUI" banner and footer markings. DoD guidance directs that this block be located at the lower right of the page. This isn't always possible. The important thing is that the block is present.

This block includes organization, office, CUI category, dissemination information, and POC information.

Please see the the CUI resource below on how to create and use the CUI "Designation Indicator Block".

5. Portion markings "(U)" and "(CUI)" (i.e., for paragraph markings) are optional when marking documents, but if used, they must be used throughout the document. Portion markings have not been used in the past when a document contains PII so recommend not using them in most cases. There may be times when they are appropriate and/or necessary.

6. Documents containing PII must only be accessible to those with an official DoD/DON need to know. This has not changed.

Transmissions of PII must be digitally signed and encrypted. This has not changed.

Note: DODI 5200.48, Controlled Unclassified Information (CUI) discusses reporting requirements if CUI is compromised (i.e. a PII breach); a new term that replaces "need to know"; a CUI cover sheet; and CUI training. The DON Privacy program should continue to follow the DoD/DON Breach Response Plans; continue to use the DoD Privacy Act Data Cover Sheet, DD Form 2923; and complete the mandatory annual DON Privacy Awareness Training. If and when changes are directed by the Defense Privacy and Civil Liberties Transparency Division (DPCLTD), this guidance will be updated.

Constructing Your CUI Designation Indicator Block

1. This block is placed on the first page of each document at the bottom right, if possible, between the header and footer CUI markings.

2. It is recommended that you create your block and save it in a convenient location so you can cut and paste it into your document when needed. At times you may need to change it slightly for the specific document, but you won't have to start from scratch.

The required elements that make up the block are:

Controlled by:
Controlled by:
CUI Category:
Distribution/Dissemination Control:
POC:

The following guidance is provided when creating your block. Remember, this is DON guidance as it relates to privacy information only as a category of CUI:

1. The first "Controlled by" line should always be "Department of the Navy" or "DON". "DON" is acceptable if it's clear to recipients that "DON" stands for "Department of the Navy".

2. The second "Controlled by" line should be how you identify your office. Some examples might be:

a. DON AA HR
b. BUPERS Code 074
c. HQMC SJA JLA

Adding "SECNAV", "NAVY" or "OPNAV", or "USMC" prior to your office information may further help identify your office.

3. The privacy CUI Category line must be one of the following privacy "sub-category" acronyms:

CONTRACT	for Contract Use
DREC	for Death Records
PRVCY	for General Privacy
GENETIC	for Genetic Information
HLTH	for Health Information
PRIIG	for Inspector General Protected
MIL	for Military Personnel Records
PERS	for Personnel Records
STUD	for Student Records

In most cases, it is recommended to use "PRVCY" which stands for "General Privacy" (see listing above). Remember, this guidance is for privacy information only. If your document contains other non-privacy categories (e.g., Legal, Financial, Law Enforcement, etc.) you would list those here also. Each of these categories have their own set of sub-categories that have their own acronyms.

4. For the "Distribution/Dissemination Control" line it is recommended that you use "FEDCON" which includes federal, military, and contractor government employees (i.e., all government employees).

Reiterating, documents containing PII should only be sent to those with an official DoD/DON need to know.

5. For the "POC" line the email originator should include their name and contact information (i.e., office email and/or office phone number). Note: When adding a CUI Designation Indicator Block to a memo, presentation, or spreadsheet, it is acceptable to make the originating office the POC since individuals come and go and the purpose is to be able to contact the originator.

An example of a complete privacy CUI Designation Indicator Block follows:

Controlled by: Department of the Navy
Controlled by: OJAG Code 13
CUI Category: PRVCY
Distribution/Dissemination Control: FEDCON
POC: CDR Jane Doe, jane.doe@navy.mil, 703-555-5555

CUI Markings for Emails containing PII

Subject line will be marked "CUI:".

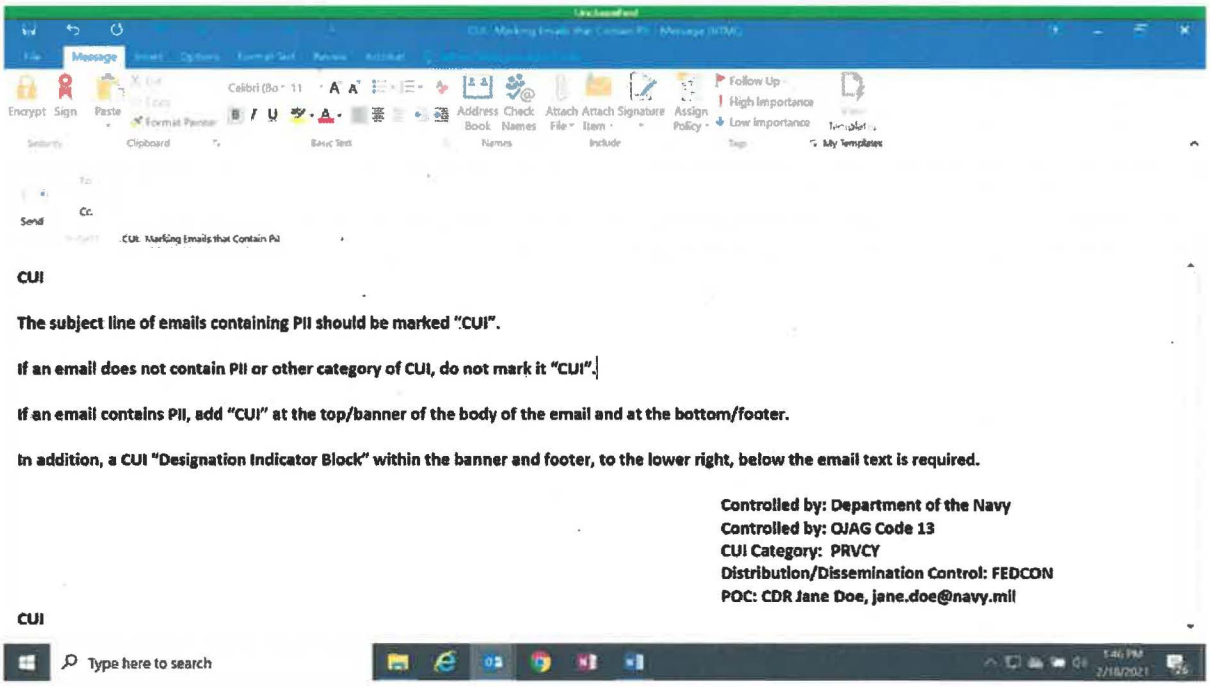
Banner (i.e., header) and footer of email body will be marked "CUI".

A CUI "Designation Indicator Block" will be added at the bottom of the email body (within the banner and footer "CUI" markings, to the right if possible. *See the additional resource page above for how to create your own Designation Indicator Block.*

Portion markings "(U)" and "(CUI)" are optional, but if used, will be used throughout the email.

If the body of an email does not contain CUI, but there is an attachment that does contain CUI, the subject line of the email should be marked "CUI". The body would not be marked. Both the attachment's file name and the document itself would be marked "CUI", and the document would have a Designation Indicator Block.

Email example:



CUI Markings for Memos Containing PII

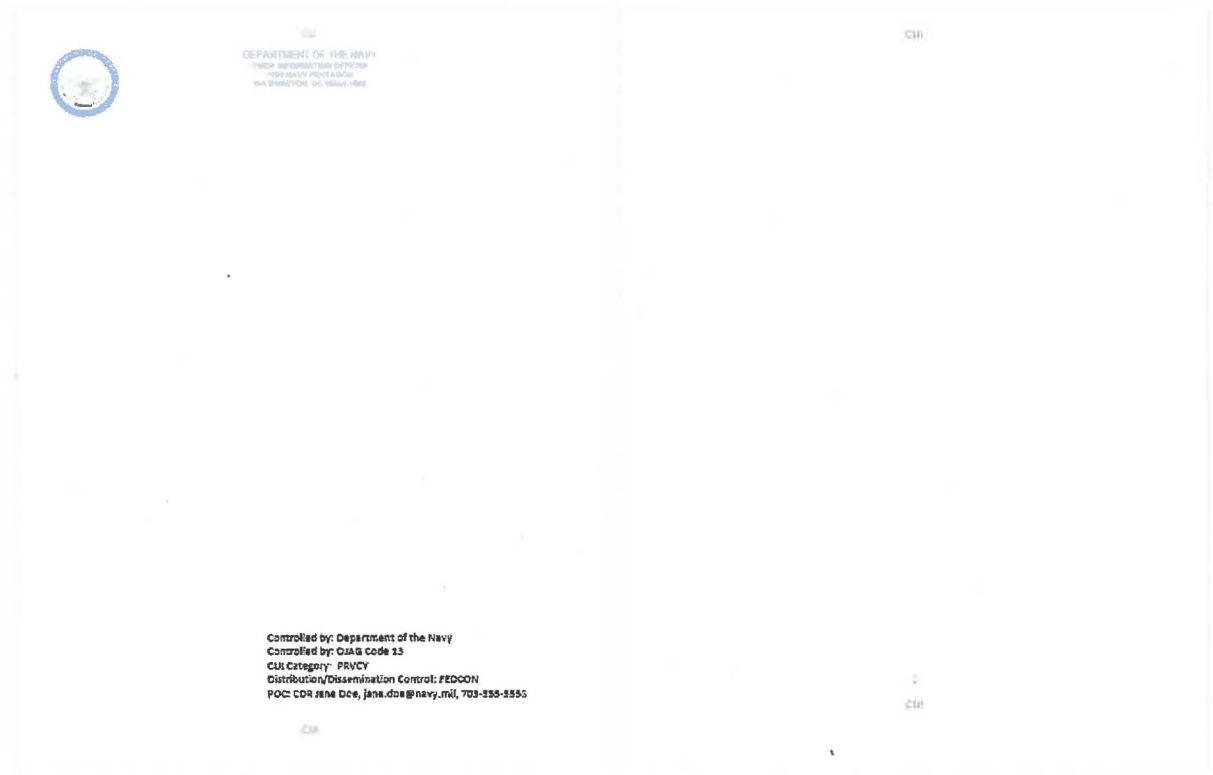
Banner (i.e., header) and footer of each page will be marked "CUI".

A CUI "Designation Indicator Block" will be added at the bottom of the first page to the lower right (within the banner and footer "CUI" markings). *See the additional resource page on creating your Designation Indicator Block above.*

Portion markings "(U)" and "(CUI)" are optional, but if used, will be used throughout the presentation.

All other pages after the first page will be marked "CUI" at the top and bottom.

Memo example:



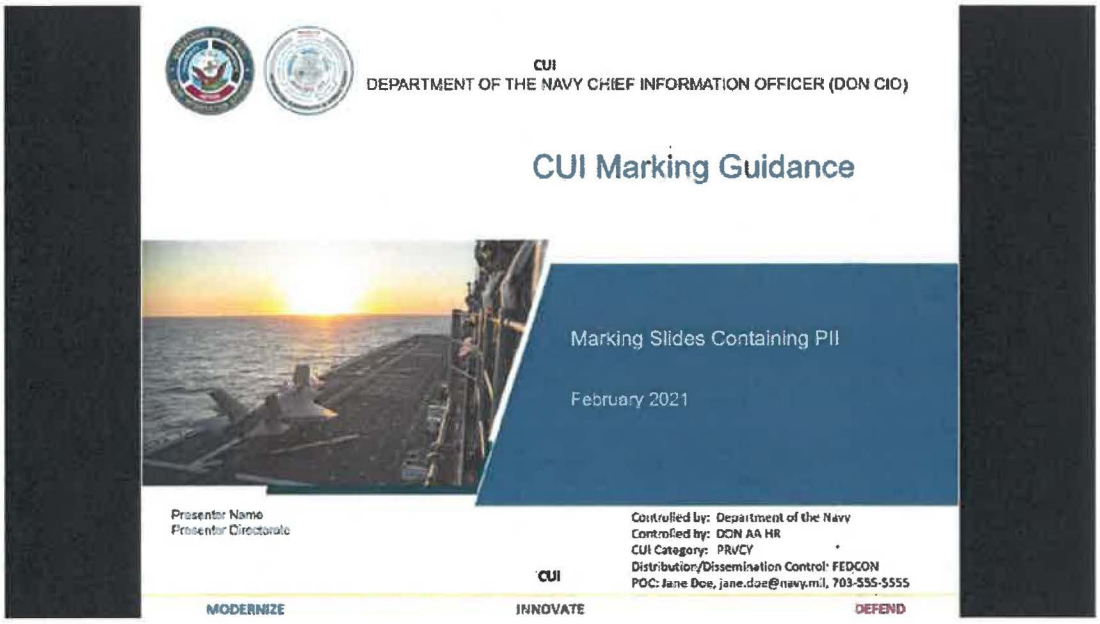
CUI Markings for Presentations (e.g., PowerPoint) Containing PII

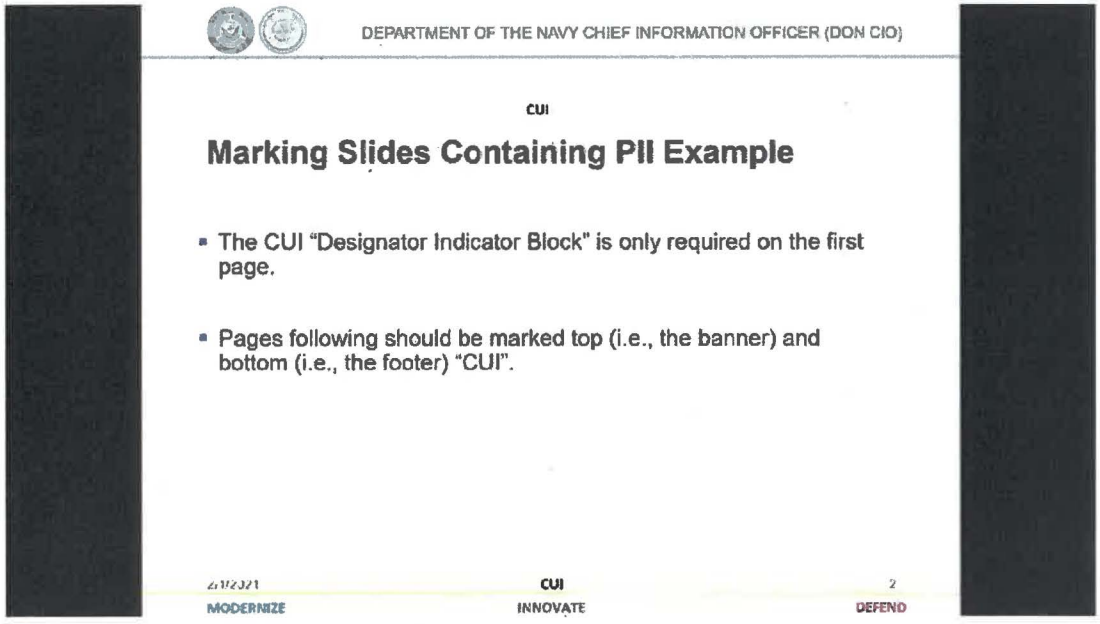
Banner (i.e., header) and footer of each page will be marked "CUI".

A CUI "Designation Indicator Block" will be added at the bottom of the first page to the lower right (within the banner and footer "CUI" markings). *See the additional resource page on creating your Designation Indicator Block above.*

Portion markings "(U)" and "(CUI)" are optional, but if used, will be used throughout the presentation.

Presentation example:





CUI Markings for Spreadsheets (e.g., Excel) Containing PII

Banner (i.e., header) and footer of each page within each tab will be marked "CUI".

A CUI "Designation Indicator Block" will be added at the bottom right of the first page of each tab containing PII (within the banner and footer "CUI" markings). *See the additional resource page on creating your Designation Indicator Block above.*

Each tab containing PII should be labeled CUI followed by the tab name.

Spreadsheets aren't as easy to mark as other documents. Please try to meet the intent.

Spreadsheet example: