DEPARTMENT OF THE NAVY -USER AGREEMENT - STANDARD MANDATORY NOTICE AND CONSENT PROVISION

By signing this document, you acknowledge and consent that when you access Department of Defense (DoD) Information Systems:

You are accessing a U.S. Government (USG) information system (IS) (which includes any device attached to this information system) that is provided for U.S. Government-authorized use only.

All users of Navy or other DoD and Federal information systems and information technology, to include but not limited to the following: desktops, laptops, virtual connections, video, teleconference, and mobility solutions (smart phones, tablets, DMCC-S), cloud applications, web applications, must adhere to the following directives for the proper use of government issued IT and information systems.

YOU CONSENT TO THE FOLLOWING CONDITIONS:

U.S. Government routinely intercepts and monitors communications on this information system for purposes including, but not limited to, penetration testing, communications security, (COMSEC) monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE) and counterintelligence (CI) investigations.

At any time, the U.S. Government may inspect and seize data stored on this information system. Communications using, or data stored on, this information system are not private, are subject to routine monitoring, interception and search, and may be disclosed or used for any U.S. Government-authorized purpose.

This information system includes security measures (authentication and access controls) to protect U.S. Government interests--not for your personal benefit or privacy.

Notwithstanding the above, using an information system does not constitute consent to personnel misconduct, law enforcement, or counterintelligence investigative searching or monitoring of the content of privileged communications or data (including work product) that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Under these circumstances, such communications and work product are private and confidential, as further explained below:

Nothing in this User Agreement shall be interpreted to limit the user's consent to, or in any other way restrict or affect, any U.S. Government actions for purposes of network administration, operation, protection, or defense, or for communications security. This includes all communications and data on an information system, regardless of any applicable privilege or confidentiality.

The user consents to interception/capture and seizure of ALL communications and data for any authorized purpose (including personnel misconduct, law enforcement, or counterintelligence investigation). However, consent to interception/capture or seizure of communications and data is not consent to the use of privileged communications or data for personnel misconduct, law enforcement, or counterintelligence investigation against any party and does not negate any applicable privilege or confidentiality that otherwise applies.

Whether any particular communication or data qualifies for the protection of a privilege, or is covered by a duty of confidentiality, is determined in accordance with established legal standards and DoD policy. Users are strongly encouraged to seek personal legal counsel on such matters prior to using an information system if the user intends to rely on the protections of a privilege or confidentiality.

Users should take reasonable steps to identify such communications or data that the user asserts are protected by any such privilege or confidentiality. However, the user's identification or assertion of a privilege or confidentiality is not sufficient to create such protection where none exists under established legal standards and DoD policy.

A user's failure to take reasonable steps to identify such communications or data as privileged or confidential does not waive the privilege or confidentiality if such protections otherwise exist under established legal standards and DoD policy. However, in such cases the U.S. Government is authorized to take reasonable actions to identify such communication or data as being subject to a privilege or confidentiality, and such actions do not negate any applicable privilege or confidentiality.

These conditions preserve the confidentiality of the communication or data, and the legal protections regarding the use and disclosure of privileged information, and thus such communications and data are private and confidential. Further, the U.S. Government shall take all reasonable measures to protect the content of captured/seized privileged communications and data to ensure they are appropriately protected.

In cases when the user has consented to content searching or monitoring of communications or data for personnel misconduct, law enforcement, or counterintelligence investigative searching, (for all communications and data other than privileged communications or data that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants), the U.S. Government may, solely at its discretion and in accordance with DoD policy, elect to apply a privilege or other restriction on the U.S. Government's otherwise-authorized use or disclosure of such information.

All of the above conditions apply regardless of whether the access or use of an information system includes the display of a Notice and Consent Banner ("banner"). When a banner is used, the banner functions to remind the user of the conditions that are set forth in this User Agreement, regardless of whether the banner describes these conditions in full detail or provides a summary of such conditions, and regardless of whether the banner expressly references this User Agreement.

USER RESPONSIBILITIES:

I understand that to ensure the confidentiality, integrity, availability, and security of Navy Information Technology (IT) resources and information, when using those resources, I shall: Safeguard information and information systems from unauthorized or inadvertent modification, disclosure, destruction, or misuse.

Protect Controlled Unclassified Information (CUI), to include Personally Identifiable Information (PII), and classified information to prevent unauthorized access, compromise, tampering, or exploitation of the information.

Protect authenticators (e.g., Password and Personal Identification Numbers (PIN)) required for logon authentication at the same classification as the highest classification of the information accessed.

Protect authentication tokens (e.g., Common Access Card (CAC), Alternate Logon Token (ALT), Personal Identity Verification (PIV), National Security Systems (NSS) tokens, etc.) at all times. Authentication tokens shall not be left unattended at any time unless properly secured. Virus-check all information, programs, and other files prior to uploading onto any Navy IT resource.

Report all security incidents including PII breaches immediately in accordance with applicable procedures.

Access only that data, control information, software, hardware, and firmware for which I am authorized access by the cognizant Department of the Navy (DON) Commanding Officer, and have a need-to-know, have the appropriate security clearance. Assume only those roles and privileges for which I am authorized.

Observe all policies and procedures governing the secure operation and authorized use of a Navy information system.

Digitally sign and encrypt e-mail in accordance with current policies.
Employ sound operations security measures in accordance with DOD, DON, service and command directives.

I FURTHER UNDERSTAND THAT, WHEN USING NAVY IT RESOURCES, I SHALL NOT:

Auto-forward any e-mail from a Navy account to commercial e-mail account (e.g, .com).
Bypass, stress, or test IA or Computer Network Defense (CND) mechanisms (Firewalls, Content Filters, Proxy Servers, Anti-Virus Programs).

Introduce or use unauthorized software, firmware, or hardware on any Navy IT resource.
Relocate or change equipment or the network connectivity of equipment without authorization from the Local IA Authority (, person responsible for the overall implementation of IA at the command level).

Use personally owned hardware, software, shareware, or public domain software without written authorization from the Local IA Authority.

Upload/download executable files (exe, .com, .vbs, or .bat) onto Navy IT resources without the written approval of the Local IA Authority.

Participate in or contribute to any activity resulting in a disruption or denial of service.
Write, code, compile, store, transmit, transfer, or Introduce malicious software, programs, or code.

Use Navy IT resources in a way that would reflect adversely on the Navy. Such uses include pornography, chain letters, unofficial advertising, soliciting or selling except on authorized bulletin boards established for such use, violation of statute or regulation, inappropriately handled classified information and PII, and other uses that are incompatible with public service.

Place data onto Navy IT resources possessing insufficient security controls to protect that data at the required classification (e.g., Secret onto Unclassified).

Digital Signature