DOD STANDARD MANDATORY

NOTICE AND CONSENT

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

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

2. You consent to the following conditions:

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

b. At any time, the U.S. Government may inspect and seize data stored on this information system.

c. 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.

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

e. 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:

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

(2) 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.

(3) 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 a 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.

(4) 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.

(5) 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.

(6) 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.

f. In cases user has consented to content searching or monitoring of communications or data for personnel misconduct, law enforcement, or counterintelligence investigative searching, (i.e., 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.

g. 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 provide a summary of such conditions, and regardless of whether the banner expressly references this User Agreement.

United States Southern Command Standard Acceptable Use Policy (AUP)

☐1. Understanding. I understand that I have the primary responsibility to safeguard the Information contained on the classified controlled unclassified and/or unclassified networks from unauthorized or inadvertent modification, disclosure, destruction, denial of service, and use.

☐2. Access. Access to this organization’s network(s) is for official use and authorized purposes and as set forth in DoD 5500.7-R, "Joint Ethics Regulation" or as further limited by this policy.

☐3. Revocability. Access to USSOUTHCOM resources is a revocable privilege and is subject to content monitoring and security testing.

☐4. Classified information processing (SIPRNet). This information system is a US-only system and approved to process classified collateral information

☐a. The classified network provides communication to external DoD organizations using the SIPRNET. Primarily done via electronic mail and internet networking protocols such as web, ftp, and telnet.

☐ b. The classified network is authorized for SECRET or lower-level processing in accordance with authorization decision.

☐ c. The classification boundary between classified network and unclassified network requires vigilance and attention by all users. The classified network is also a US and US-sponsored only system and not accredited for transmission of NATO material.

☐ d. CONFIDENTIAL information must be processed at the SECRET or higher level.

☐ e. The ultimate responsibility for ensuring the protection of information lies with the user. The release of TOP SECRET information through the classified network is a security violation and will be investigated and handled as a security violation or as a criminal offense.

☐ 5. Controlled and Unclassified Information Processing (NIPRNet). The Unclassified Network is the primary controlled unclassified and unclassified automated administration tool for USSOUTHCOM. The NIPRNet is a US and US-sponsored only system. The NIPRNet is approved to process UNCLASSIFIED and SENSITIVE information, in accordance with local regulations dealing with automated information system security management programs.

☐ a. The NIPRNet provides unclassified communication to external DoD and other United States Government organizations. Primarily done via electronic mail and internet networking protocols such as web, File Transfer Protocol (FTP), telnet.

☐ b. The NIPRNet network is approved to process UNCLASSIFIED and SENSITIVE (encrypted PII, HIPAA, agency-sensitive data that does not rise to the level of classified, but is required protection by federal statutes). CONFIDENTIAL information is not processed or stored on the NIPRNet.

☐ c. The ultimate responsibility for ensuring the protection of information lies with the user. The release of CONFIDENTIAL or higher information through the unclassified network is a security violation and will be investigated and handled as a security violation or as a criminal offense

☐ 6. The SOUTHCOM Public Internet Access Network (SPIAN) is a government, official use only Internet domain. SPIAN use supports partners that do not meet the requirements for US-sponsored access to NIPRNet and other validated agency missions. It is not a morale, welfare and recreation (MWR) domain for personal use.

☐ 7. All USSOUTHCOM networks (SIPRNet, NIPRNet, and SPIAN) are monitored IAW DOD policy

☐ 8. Minimum security rules and requirements. As a SIPRNet, NIPRNet, or SPIAN Network system user, the following minimum-security rules and requirements apply:

☐ a. DOD personnel security and vetting requirements for network access. Access to SPIAN requires validated justification.

☐ b. Initial user Cybersecurity awareness training and annual Cybersecurity awareness training, must be completed, as a prerequisite for continuous network access. SOUTHCOM utilizes the Learning Management System (LMS) to track this requirement. However, the Cyber Awareness Challenge course is also available through Joint Knowledge Online (JKO) and Defense Information Systems Agency (DISA) portal located at https://cyber.mil. Participation in all training programs, as required, inclusive of additional DOD and organizational supplementary education and awareness training is required (e.g. corrective training, threat identification, physical security, acceptable use policies, malicious content and logic identification, and nonstandard threats, such as, social engineering).

☐ c. I will ensure my CAC and SIPRNet NSS token are removed from machines when I am not in immediate proximity. I will not share my CAC/NSS pins. User accounts are authenticated through Public

Key Infrastructure (PKI) when connected to USSOUTHCOM's network, under user-role based permissions managed by the site in Active Directory (AD).

☐**d. I will use only authorized hardware and software. I will not install or use any personally owned hardware, software, shareware, or public domain software, including removable devices of any kind (such as USB, phones-USG or personal). Removable or mobile devices are not authorized under any circumstances, not even to recharge. From its first established connection, whether intentional or not, these devices pose a threat of introducing malware.**

☐e. I will use virus-checking procedures before uploading or accessing information from any system, diskette, attachment, or compact disk.

☐f. I will not attempt to access or process data exceeding the authorized IS classification level.

☐g. I will not alter, change, configure, or use operating systems or programs, except as specifically authorized.

☐h. I will not introduce executable code (such as, but not limited to, .exe, .com, .vbs, or .bat files) without authorization, nor will I write any code.

☐i. I will safeguard and mark with the appropriate classification level all information created, copied, stored, or disseminated from the IS and will not disseminate it to anyone without a specific need to know.

☐j. I will not utilize USSOUTHCOM- or DoD-provided ISs for commercial financial gain or illegal activities.

☐k. Maintenance will be performed by the System Administrator (SA) only.

☐l. I will use screen locks and log off the workstation when departing the area.

☐m. I will immediately report any suspicious output, files, shortcuts, or system problems to the Organization's System Administrator and/or Information Systems Security Manager (ISSM) or Information Systems Security Officer (ISSO) and cease all activities on the system.

☐n. I will address any questions regarding policy, responsibilities, and duties to the organization's System Administrator and/or site ISSM/ISSO.

☐o. I understand that each IS is the property of USSOUTHCOM and is provided to me for official and authorized use. I further understand that each IS is subject to monitoring for security purposes and to ensure that use is authorized. I understand that I do not have a recognized expectation of privacy in official data on the IS and may have only a limited expectation of privacy in personal data on the IS. I realize that I should not store data on the IS that I do not want others to see.

☐p. I understand that monitoring of classified and unclassified networks shall be conducted for various purposes and information captured during monitoring may be used for administrative or disciplinary actions or for criminal prosecution. I understand that the following activities define unacceptable use of an USSOUTHCOM's IS:

☐• to show what is not acceptable use

☐• to show what is acceptable during duty/non-duty hours

☐• to show what is deemed proprietary or not releasable (key word, classification or data identification)

☐• to show what is deemed unethical (e.g., spam, profanity, sexual content, gaming)

☐ • to show unauthorized sites (e.g., pornography, streaming video, E-Bay)

☐ • to show unauthorized services (e.g., peer-to-peer, distributed computing)

☐ • to define proper email use and restrictions (e.g., mass mailing, hoaxes, auto forwarding)

☐ • to explain expected results of policy violations (1st, 2nd, 3rd, etc.) (Note: Activity in any criteria can lead to criminal offenses.) 1st Offense: retraining, 2-day suspension of network access, and counseling by immediate supervisor; 2nd Offense: 7-day suspension of network access, retraining, and Director/commander (O-6 or higher) level counseling; 3rd Offense: 30-day suspension, retraining & violation stored in local PERSEC file.

☐ q. The information below will be used to identify you and may be disclosed to law enforcement authorities for investigating or prosecuting violations. Disclosure of information is voluntary; however, failure to disclose information could result in denial of access to the organization's information systems.

☐ 9. Acknowledgement. I have read the above requirements regarding use of this organization's access systems. I understand my responsibilities regarding these systems and the information contained in them.

Last Name: _____

First Name: _____

Initial: _____

Signature Field:

Grade/Series/Contractor:

Site/Directorate/Division: _____

Date/Time Field: _____