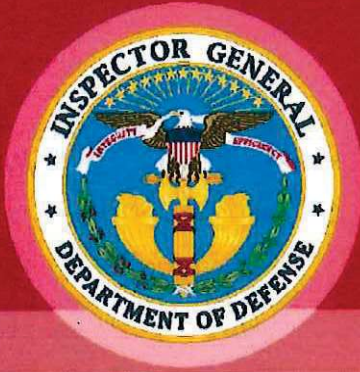


~~SECRET//NOFORN~~

Report No. DODIG-2022-076



INSPECTOR GENERAL

U.S. Department of Defense

March 28, 2022

(U) Evaluation of Combatant Commands' Communication Challenges with Foreign Partner Nations during Coronavirus Disease-2019 Pandemic and Mitigation Efforts

Classified By: DODIG (b)(6)

Contingency Operations, Evaluations
Derived From: Multiple Sources

Declassify On: 2047-04-28

This content is classified at the ~~SECRET//NOFORN~~ level and may contain elements of controlled unclassified information (CUI), unclassified information classified at a lower level than the overall classification displayed. This content shall not be used as a source of derivative classification, referred to in the applicable classification guide. It must be reviewed for both Classified National Security Information (CNSI) and CUI in accordance with DoD 5230.09 prior to public release.

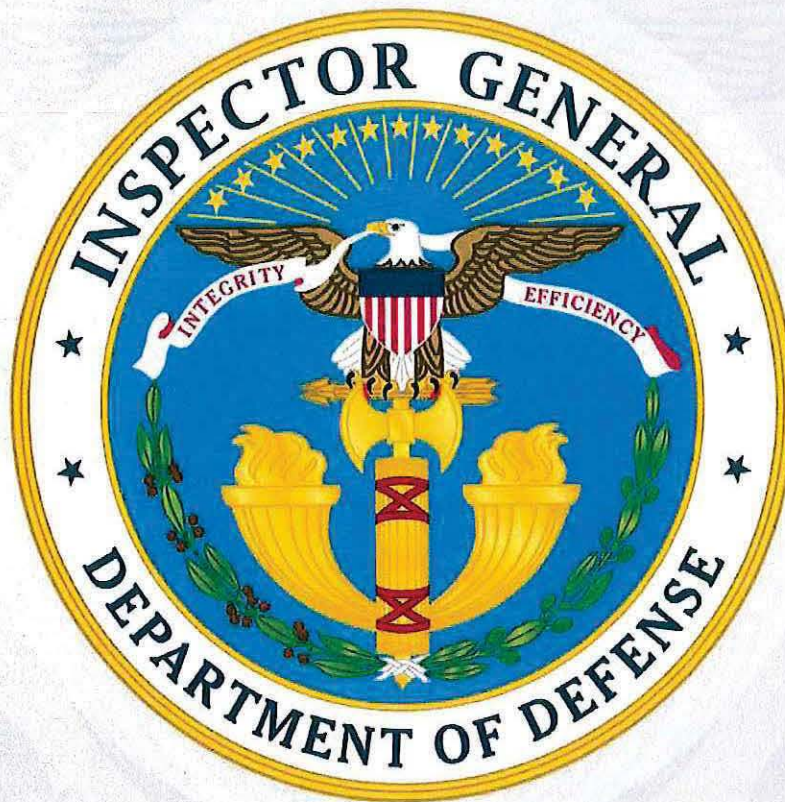
Overseas

INTEGRITY ★ INDEPENDENCE ★ EXCELLENCE

~~SECRET//NOFORN~~

"Released by the DoD OIG
FOIA Office under FOIA
request
DODOIG-2022-000666 on
June 13, 2024"

~~SECRET//NOFORN~~



~~SECRET//NOFORN~~

~~SECRET/NOFORN~~



INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
4800 MARK CENTER DRIVE
ALEXANDRIA, VIRGINIA 22350-1500

March 28, 2022

MEMORANDUM FOR UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE
AND SECURITY

CHIEF INFORMATION OFFICER OF THE DEPARTMENT
OF DEFENSE

COMMANDER, UNITED STATES AFRICA COMMAND

COMMANDER, UNITED STATES CENTRAL COMMAND

COMMANDER, UNITED STATES EUROPEAN COMMAND

COMMANDER, UNITED STATES

INDO-PACIFIC COMMAND

COMMANDER, UNITED STATES SOUTHERN COMMAND

SUBJECT: Evaluation of Combatant Commands' Communication Challenges
with Foreign Partner Nations during the Coronavirus
Disease -2019 Pandemic and Mitigation Efforts
(Report No. DODIG-2022-076)

(U) This final report provides the results of the DoD Office of Inspector General's evaluation. We provided copies of the draft report and requested written comments on the recommendations. We considered management's comments on the draft report when preparing the final report. These comments are included in the report.

(U) This report contains a total of 7 recommendations, of which, 6 recommendations are considered resolved, but open. Specifically, the DoD Chief Information Officer, the Under Secretary of Defense for Intelligence and Security, the U.S. Africa Command Commander, the U.S. Central Command Commander, the U.S. European Command Commander, and the U.S. Southern Command Commander agreed to the recommendations presented in the report and provided a plan of action. Therefore, we consider the recommendations resolved and open. This report also contains one recommendation that is unresolved. Specifically, the U.S. Indo-Pacific Command Commander did not respond to the recommendations in the report. Therefore, the recommendation is unresolved. We request that the USINDOPACOM Commander provide comments on the final report.

~~SECRET/NOFORN~~

~~SECRET/NOFORN~~

(U) DoD Instruction 7650.03 requires recommendations be resolved promptly. Therefore, please provide us within 30 days your response concerning specific actions in process or alternative corrective actions proposed on the recommendations. If you have any questions, or would like to discuss the evaluation, please contact me at [REDACTED] (DSN [REDACTED]).

Bryan T. Clark

Bryan T. Clark
Acting Assistant Inspector General for
Evaluations, Programs, Combatant
Commands, and Overseas Contingency
Operations

~~SECRET/NOFORN~~

(U) Objective

(U) The objective of this evaluation was to determine how the U.S. Africa Command (USAFRICOM), the U.S. Central Command (USCENTCOM), the U.S. European Command (USEUCOM), the U.S. Indo-Pacific Command (USINDOPACOM), the U.S. Southern Command (USSOUTHCOM), and their component commands mitigated communication problems with partner nations during the coronavirus disease-2019 (COVID-19) pandemic and how these mitigation strategies should be employed in future operations where face-to-face interaction is not possible.

(U) Executive Summary

(U) We determined how USAFRICOM, USCENTCOM, USEUCOM, USINDOPACOM, USSOUTHCOM, and their component commands mitigated communication problems with partner nations during the COVID-19 pandemic.

(S) NDOPACOM (b)(1)1.4a
[Redacted text block]

(S) NDOPACOM (b)(1)1.4a
[Redacted text block]

(U) Background

(U) DoD Response to COVID-19

(U) Since January 2020, the DoD has developed strategies to protect the health of service members from COVID-19, with a goal of minimizing risks while continuing operations. The DoD has issued force health protection guidance and supplements since January 30, 2020 on a range of topics that include risk reduction measures, testing, treatment, and travel. In March 2020, the Secretary of Defense imposed DoD-wide stop movement orders. In response to these measures, the CCMDs and many of their partner nations (PNs) imposed travel restrictions, border closures, and quarantine mandates, which prevented face-to-face interactions and travel into and within the CCMDs' respective areas of responsibility (AORs).

(U) Between September 2020 and April 2021, the DoD OIG issued five evaluations related to CCMDs' responses to the COVID-19 pandemic—one on USAFRICOM, one on USCENTCOM, one on USEUCOM, one on USINDOPACOM, and one on USSOUTHCOM.

(U) These reports addressed how the CCMDs and their respective component commands executed their pandemic response plans and continuity of operations plans to mitigate the impact of COVID-19 on operations. Each report provided details about the respective CCMD's implementation of large-scale telework, along with the importance of telework infrastructure (hardware and software). These reports also highlighted communication challenges between the CCMDs and PNs during the COVID-19 pandemic.

(U) DoD Communication Policies and Tools

(U) According to Joint Publication 3-16, the success of joint and multinational operations and interagency coordination hinges upon timely and accurate information and intelligence sharing.¹ An intelligence and information sharing environment that fully integrates joint, multinational, and interagency partners in a collaborative enterprise enables information sharing, cooperation, collaboration, and coordination. The joint force commander participating in the coalition or alliance tailors the communications policy and procedures for that particular operation based on national and theater guidance.

(U) DoD Policy for Electronic Messaging, Records Management, and Operations Security (OPSEC)

(U) DoD Instruction (DoDI) 8170.01 establishes policy, assigns responsibilities, and prescribes procedures for conducting, establishing, operating, and maintaining electronic messaging services (including, but not limited to, e-mail) to collect, distribute, store, and otherwise process unclassified and classified official DoD information.² Specifically, DoDI 8170.01 prohibits DoD personnel from using personal e-mail or other nonofficial accounts to exchange official information and from auto-forwarding official messages to nonofficial accounts.³ DoDI 8170.01 also states that employees may not use personal, nonofficial accounts to conduct official DoD communication for personal convenience or preference. Additionally, the DoDI states "DoD personnel may not use personal, nonofficial accounts, to conduct official DoD communications" and must meet three combined conditions to qualify for an exception. The three conditions are:

1. (U) Emergencies and other critical mission needs.
2. (U) When official communication capabilities are unavailable, impractical, or unreliable.
3. (U) It is in the interests of DoD or other U.S. government missions.

¹ (U) Joint Publication 3-16, "Multinational Operations," March 1, 2019, Validated on February 12, 2021.

² (U) DoDI 8170.01, "Online Information Management and Electronic Messaging," January 2, 2019.

³ (U) "The DoD Dictionary of Military and Associated Terms," August 2021, defines official information as information that is owned by, produced for or by, or is subject to the control of the U.S. Government.

(U) A DoD Chief Information Officer (CIO) memorandum about authorized telework capabilities and guidance issued on April 13, 2020, stated that DoD components should first consider using DoD Enterprise Collaboration Capabilities, then consider commercial services that have a DoD Provisional Authorization, and if neither of these are able to meet the component's needs, submit their requirements for approval to the DoD CIO and the U.S. Cyber Command.⁴ The memorandum provided a list of DoD-provided and provisionally authorized commercial services in an appendix and directed personnel to an updated list available online.⁵

(U) DoDI 5015.02 establishes policy and assigns responsibilities for the management of DoD information "created, received, collected, processed, maintained, disseminated, disclosed, or disposed of by or for the DoD, in any medium or form, including information managed by DoD or a third party on behalf of DoD."⁶ The Instruction also states that DoD personnel is prohibited from using (with very few exceptions) nonofficial electronic messaging accounts to conduct official DoD communication. In the instances where an employee must use nonofficial electronic messaging accounts, he or she must "copy the message to his or her official electronic messaging account when the record is first transmitted, or must forward a complete copy of the record to their official electronic messaging account within 20 days of the record's original creation or transmission."

(U) DoD Directive (DoDD) 5205.02E establishes policy and responsibilities governing the DoD OPSEC program.⁷ Specifically, DoDD 5205.02E states that OPSEC must be considered across all DoD missions, functions, programs, and activities. The Directive also states that DoD personnel must maintain essential secrecy of information that is useful to adversaries and potential adversaries to plan, prepare, and conduct military and other operations against the United States and shall safeguard such information from unauthorized access and disclosure. Finally, the Directive directs combatant commanders to integrate OPSEC into all contingency planning and operations and "develop area specific OPSEC training for deploying Service members to complete prior to arrival in theater."

(U) The Mission Partner Environment

(U) The DoD created a suite of capabilities known as the Mission Partner Environment (MPE) that enables the joint force to share information and exchange data with mission partners through all phases of operations. The MPE is an operating environment that enables command and control for operational support planning and execution on a network infrastructure at a single security level with a common language

⁴ (U) DoD CIO Memorandum, "Authorized Telework Capabilities and Guidance," April 13, 2020.

⁵ (U) The memorandum directed personnel to <https://cyber.mil/covid19> to find the updated list.

⁶ (U) DoDI 5015.02, "DoD Records Management Program," February 24, 2015 (Incorporating Change 1, August 17, 2017).

⁷ (U) DoDD 5205.02E, "DoD Operations Security (OPSEC) Program," June 20, 2012 (Incorporating Change 2, August 20, 2020).

~~SECRET/NOFORN~~

(U) and enables mission partners to share their information with all participants within a specific partnership or coalition throughout an operation.

(U) The Secretary of the Air Force is the DoD's executive agent for MPE and relies on the Administrative Assistant to the Secretary of the Air Force (SAF/AA) Mission Partner Capability Office (MPCO) to administer the MPE for all of the DoD. The SAF/AA MPCO directly manages:

1. (U) a Virtual Data Center to provide multi-enclave virtualizations and host multiple discreet mission enclaves and networks;
2. (U) CENTRIXS mission enclaves that allow U.S. and coalition nations and forces to securely share operational and intelligence information;
3. (U) Pegasus, the Five Eye Nation classified information sharing network;
4. (U) CFBLNET, a research, development, test, and evaluation environment for the United States and its PN's;
5. (U) the All Partners Access Network, a DoD unclassified information sharing and collaboration service that is accessible to individuals and organizations without access to traditional DoD systems and networks;
6. (U) the United States Battlefield Information Collection and Exploitation System, the classified collaborative information and intelligence sharing system for North Atlantic Treaty Organization (NATO) Allies and seven non-NATO nations; and
7. (U) the United States Battlefield Information Collection and Exploitation System Extended (BICES-X) that provides classified collaborative information and intelligence sharing systems to CCMDs based on their specific intelligence sharing needs. Some of these systems have AOR-specific names like the USCENTCOM Partner Network or Asia-Pacific Intelligence Information Network.

(S//REL USA, FVEY) ~~INDOPACOM (b)(1)1.4a~~

⁸(U) Joint Chiefs of Staff "COVID-19 Military Response In-Stride Review: Consolidated Report," Report Classified SECRET/NOFORN Declassify on 20450826.

(U) This report consolidated findings, insights, and recommended actions from the in-stride review of the military response to the coronavirus 2019 (COVID-19) pandemic. The Chairman directed the review to improve the Joint Force's ability to effectively respond to a global pandemic and other strategic challenge. This report synthesizes strategic insights and challenges discovered and encountered by the combatant commands, Services, National Guard Bureau, and the Joint Staff. The Services, National Guard Bureau, and several combatant commands produced individual after action reports forwarded under separate correspondence.

~~SECRET/NOFORN~~

(S//REL USA, FVEY) [NDOPACOM (b)(1)1.4a]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

(U) Combatant Commands and Their Component Commands

(U) This evaluation focused on foreign partner communication and collaboration conducted by the following five CCMDs: USAFRICOM, USCENTCOM, USEUCOM, USINDOPACOM, and USSOUTHCOM. The Doctrine for the Armed Forces of the United States in Joint Publication 1 describes the role of the geographic CCMDs as:

(U) The vital link between those who determine national security policy and strategy and the military forces or subordinate Joint Force Commanders that conduct military operations within their areas of responsibility. [Geographic CCMDs] are responsible for a large geographical area and for effective coordination of operations within that area.

(U) CCMD desk officers often lead country planning and work directly with the senior defense officials or defense attachés in their AORs and their counterparts in the Service component commands to develop country-level plans and identify forces and resource requirements. The Service component commands prepare supporting objectives and plans and may include organize, train, and equip responsibilities such as exercises, readiness, interoperability, augmentation, joint enablers, and capabilities development. Theater special operations commands coordinate special operations integration and Service component support of special operations for special operations core activities in all campaigns and operations. Theater special operations commands also support special operations forces conducting security force assistance activities and other security cooperation activities in support of the geographic CCMDs.

(U) Other Key DoD Components Involved in Foreign Partner Communications Policy or Execution

(U) Under Secretary of Defense for Intelligence and Security (USD[I&S])

(U) The USD(I&S) is the principal staff assistant and advisor to the Secretary of Defense and Deputy Secretary of Defense on intelligence, counterintelligence, security, sensitive activities, and other intelligence-related matters and exercises planning, policy, and strategic oversight over all DoD intelligence, counterintelligence, and security policy, plans, and programs.

(U) DoD Chief Information Officer (CIO)

(U) The DoD CIO is the principal staff assistant and advisor to the Secretary of Defense and Deputy Secretary of Defense for information technology, information resources management, and efficiencies and also responsible for all matters relating to the DoD information enterprise such as cybersecurity, communications, information systems, and more.

(U) National Guard Bureau (NGB) State Partnership Program (SPP)

(U) The NGB's SPP supports the security cooperation objectives of the U.S. and geographic CCMDs by developing enduring relationships with partner countries and carrying out activities to build partner capacity, improve interoperability, and enhance U.S. access and influence while increasing the readiness of U.S. and partner forces to meet emerging challenges. The SPP has paired every U.S. state and territory with at least one partner nation. There are at least 82 partnerships and 1,000 events annually.

(U) Available DoD Tools Did Not Meet All CCMD Needs Because of Foreign Partner Limitations

~~(S//NF)~~

NDOPACOM (b)(1)1.4a

[REDACTED]

(U) Foreign Partners' Technological, Cultural, and Computer Literacy Limitations Impacted Communications During COVID-19

(U) Foreign partners' technological, cultural, and computer literacy limitations impacted CCMD personnel's ability to communicate during the pandemic. Many CCMD personnel told us that their partners had technological challenges during the COVID-19 pandemic, such as limited internet access or bandwidth, especially in rural areas. This necessitated that CCMDs operate within their foreign partner's limitations while also being sensitive to their cultural preferences.

~~(S//NF)~~ For example, USAFRICOM staff personnel highlighted challenges some African partners have in reaching U.S. standards for information sharing systems, which limited the tools available to communicate during the COVID-19 pandemic. One staff member explained that

AFRICOM (b)(1)1.4a

[REDACTED] that some partner nations could not provide. Another staff member provided the example of a partner's

AFRICOM (b)(1)1.4d

[REDACTED] by U.S. standards. The staff member pointed out how unrealistic it was for some of these partners to be able to meet facilities and security standards for U.S. equipment, especially during the COVID-19 pandemic.

~~(S//NF)~~ CCMD personnel also described cultural barriers that impeded communications while operating in the virtual environment. A USCENTCOM staff member explained the importance of personal relationships and that the cultural bias of some foreign partners is that "if [the meeting] is not face-to-face, you can't hold me to [what was agreed to]." USCENTCOM personnel stated that when they held virtual meetings, there was a lack of interaction and the meetings were not as productive. For example, a USCENTCOM staff member explained that in accordance with controlled information sharing memoranda agreements between the command and PNs, there were a specific number of required meetings that needed to take place in order to share controlled information with PNs. The meetings were held virtually because of COVID-19 and after the first set of virtual meetings, not a single country came back for a subsequent virtual event. Only three of the 10 countries had met the number of required meetings for 2020, and only five of 10 countries will achieve the meeting requirements for 2021. Similarly, USAFRICOM personnel described challenges with their ~~AFRICOM (b)(1)(1).4d~~

~~(S)~~ Computer literacy was also a barrier for some foreign partners. For example, one USCENTCOM representative explained that computer usage in one PN is different because many mid to senior officers do not use computers themselves or know their username and password for their computers or the CENTCOM Partner Network. Several CCMD personnel told us that their foreign partners were more skilled with or preferred mobile technology (mobile phones) to computers. However, many DoD-provided capabilities are computer-based, not mobile phone-based.

(U) DoD's Commercial Virtual Remote Environment Supported Communications With Foreign Partners Until June 2021

(U) In addition, one tool that CCMD personnel told us they relied on to communicate with U.S. and foreign partners was the Commercial Virtual Remote (CVR) environment, a temporary capability to provide Microsoft Teams and a cloud environment to the DoD during maximum telework. However, the DoD eliminated CVR in June 2021 because it did not meet the cybersecurity requirements for Controlled Unclassified Information (CUI).

(U) The DoD made the CVR environment available to help support communication and collaboration during the pandemic response, but eliminated the capability in June 2021 as they introduced a new DoD365 environment. One CCMD staff member said losing the CVR capability "severely inhibited our ability to do our functions," a sentiment shared by personnel across the CCMDs. We asked the Office of the DoD CIO why CVR was eliminated and replaced with DoD365. The response from the Office of the DoD CIO explained that:

(U) The CVR (Teams and One Drive) environment was always meant to be temporary and was extended twice to allow for an orderly,

(U) methodical, and planned transition to the DoD365 environment. The two main driving factors in why CVR could not be extended any further was the cybersecurity risk & the cost of maintaining a second (commercial) environment. CVR lacked the full set of required capabilities and security features to support the Department's controlled unclassified information (CUI) requirements.

(U) Personnel from across the CCMDs complained about the lack of key capabilities, like a conference bridge line and partner accessibility between CVR and DoD365. The NGB SPP response to our request for information described the transition to DoD365 and its requirement for a common access card to access Microsoft Teams as a major setback for SPP virtual engagements. They said that this transition limited the states' ability to invite partners as guests to the platform and further restricted cross-component collaboration.

(S) INDPACOM (b)(1)1.4a
[REDACTED]

(S) NDOPACOM / AFRICOM (b)(1)1.4a
[REDACTED]

(U) AFRICOM (b)(1)1.7e
[REDACTED]
(U) AFRICOM (b)(1)1.7e
[REDACTED]
(U) AFRICOM (b)(1)1.7e
[REDACTED]
(U) AFRICOM (b)(1)1.7e
[REDACTED]
(U) AFRICOM (b)(1)1.7e
[REDACTED]
(U) AFRICOM (b)(1)1.7e
[REDACTED]

(S) NDOPACOM (b)(1)1.4a
[REDACTED]

(S) NDOPACOM (b)(1)1.4a
[REDACTED]

(U) CCMDs Did Not Comply With Records Management Policy

(U) DoD policies, along with a 2015 DoD CIO-issued memorandum, describe the records management requirements that DoD personnel who use any non-official electronic messaging account to conduct official business must follow. DoD policies direct that such personnel must copy the message to their official electronic messaging account at the time of creation, or within 20 days after transmitting the original message.¹⁰

(U) DoDI 8170.01 states that DoD and OSD component heads are responsible for ensuring that all nonpublic DoD information is collected, distributed, shared, stored, or otherwise processed on systems that comply with DoDIs 8510.01 and 8582.01, and DoD 5220.22-M. Combatant commanders must ensure that their commands preserve records in accordance with policy and law.

(S) NDOPACOM (b)(1)1.4a / EUCOM (b)(1)1.4g
[REDACTED]

¹⁰ (U) DoDI 5015.02, "DoD Records Management Program," February 24, 2015 (Incorporating Change 1, August 17, 2017).

(U) DoDI 8550.01, "DoD Internet Services and Internet-Based Capabilities," September 11, 2012.

(U) DoDI 5200.48, "Controlled Unclassified Information (CUI)," March 6, 2020.

(U) DoD CIO Memorandum, "Use of Non-Official Electronic Messaging Accounts and Records Management," April 6, 2015.

(S)

NDOPACOM (b)(1)1.4a

(S)

NDOPACOM (b)(1)1.4a / AFRICOM (b)(1)1.4g

(U) DoDI 8170.01 assigns several electronic messaging and OPSEC related responsibilities to the USD(I&S). The USD(I&S) is responsible for:

- (U) monitoring and ensuring cybersecurity and OPSEC vulnerabilities found on electronic messaging services are identified and resolved;
- (U) coordinating corrective action for DoD electronic messaging services not operated in compliance with applicable cybersecurity and OPSEC policies with the responsible DoD and OSD component heads and the DoD CIO;
- (U) integrating guidance regarding the responsible and effective use of electronic messaging services in OPSEC education, training, and awareness activities; and
- (U) establishing guidance for protecting controlled unclassified information in coordination with controlled unclassified information legal, regulatory and regulatory guidelines.

(U) Similarly, DoDI 8170.01 assigns several electronic messaging and OPSEC-related responsibilities to the combatant commanders as DoD component heads. The Instruction states that the combatant commanders are responsible for ensuring that:

¹¹ (U) Report No. DODIG-2021-065, "Evaluation of Access to Department of Defense Information Technology and Communications During the Coronavirus Disease-2019 Pandemic," April 1, 2021.

(U) 1) subordinate component personnel are educated and trained in the responsible and effective use of electronic messaging services, including accessibility, OPSEC, cybersecurity, records management, and information review for clearance and release authorization procedures; 2) all electronic messaging services used by the component to distribute DoD information are assessed at least annually for compliance with DoDI 8170.01; and 3) DoD cybersecurity standards, controls, and enforcement are maintained.

~~(CUI)~~ In July 2020, the Secretary of Defense directed the USD(I&S) to conduct a coordinated OPSEC campaign. As part of that campaign, the Office of the USD(I&S) conducted a review of its OPSEC program and found that nearly half of DoD components stated they did not conduct pre-deployment OPSEC training, as required by DoDD 5205.02E. Additionally, during the review a number of DoD components stated to the Office of the USD(I&S) that fewer than 75 percent of personnel are trained on the organization's critical information and indicators, with other respondents stating fewer than 25 percent of personnel are. These training gaps increase the risk that component personnel do not know what types of information must be protected against unauthorized disclosures.

~~(CUI)~~ On June 22, 2021, the Office of the USD(I&S) issued a memorandum for senior Pentagon leadership, the combatant commanders, and Defense agency and field activity directors requesting their assistance to ensure their information security and OPSEC programs had safeguards to prevent unauthorized disclosures such as posting non-public information to a closed group on a commercial social media platform even if all members of the group are otherwise authorized to receive the information. CCMD personnel responses during our interviews, conducted in August and September 2021, and the findings of the OPSEC program review suggest that the Office of the USD(I&S) and the CCMDs should develop policy to mitigate the risk of using non-DoD-controlled electronic messaging systems and develop additional OPSEC training requirements on the risks of sharing DoD information on non-DoD-controlled systems to meet their responsibilities as directed in DoDI 8170.01.

(U) USCENTCOM Regulation Authorized Use of Non-DoD-Controlled Electronic Messaging Systems Despite DoD Policy

(U) A 2018 Deputy Secretary of Defense memorandum for all DoD personnel states that

Law and DoD policy are clear: 'non-official electronic messaging accounts,' including personal email accounts, must not be used to conduct official DoD communications, with very few exceptions... Personal or other non-official email accounts may be used for official

(U) business only in those rare and extraordinary situations where an official email capability is not available.¹²

(U) DoDI 8170.01 reiterates the prohibition, unless all three exception criteria are met. DoDI 8170.01 paragraph 3.24 specifically cautions DoD personnel to not use non-DoD-controlled electronic messaging services to process non-public DoD information, regardless of the service's perceived appearance of security (for example, "private" Instagram accounts, "protected" tweets, "private" Facebook groups, and "encrypted" WhatsApp messages). Additionally, on March 19, 2020, as the DoD was implementing maximum telework, the DoD CIO's Chief of Staff distributed refresher "do's" and "don'ts" cybersecurity guidance that said, "[Do Not] use any non-DoD instant messaging applications to share DoD information."

(S) CENTCOM (b)(1)1.7e
[REDACTED]

(U) CCMDs must balance both their operational need to remain engaged with partners, using communication tools available and accessible to the PN, and the requirement to comply with DoD policy. DoDI 8170.01 affirms that "it is DoD policy that DoD personnel must continue to innovate via electronic messaging services to achieve capabilities that are faster, better and less expensive, while simultaneously ensuring implementation of cybersecurity appropriate for the risks, and the magnitude of harm that could result from the loss, compromise, or corruption of the information." Although DoDI 8170.01 provides exception criteria, it does not provide a mechanism or specific parameters for exercising the exception.

¹² (U) Deputy Secretary of Defense Memorandum for All Department of Defense Personnel, "Conducting Official Business on Electronic Messaging Accounts," January 16, 2018.

¹³ (U) Central Command Regulation 380-8, "Cybersecurity and Support to Defensive Cyberspace operations," February 5, 2021.

(U) Due to the increased risk, the difficulty of complying with records management requirements, and the lack of established policy for using non-DoD-controlled electronic messaging systems, USAFRICOM, USCENTCOM, USEUCOM, USINDOPACOM, and USSOUTHCOM should issue policy clarifying the requirements for any use of non-DoD-controlled electronic messaging systems and provide specific guidance on how to use them for communicating with PN and establish risk assessment procedures to evaluate and monitor CCMD use of current and emerging information technologies to identify opportunities for use and to assess risks.

(U) Challenges With Sharing Classified Information During the COVID-19 Pandemic

(S//NF) EUCOM (b)(1)1.4g

[REDACTED]

(S//NF) AFRICOM (b)(1)1.4g / EUCOM (b)(1)1.4g / NDOPACOM (b)(1)1.4a

[REDACTED]

(U) Increased Opportunities for U.S. Adversaries to Exploit Communication Vulnerabilities

(S//REL TO USA, FVEY) AFRICOM (b)(1)1.4g / CENTCOM (b)(1)1.4a, (b)(1)1.4g / INDOPACOM (b)(1)1.4a

[REDACTED]

(S//REL TO USA, FVEY) CENTCOM (b)(1)1.4a, (b)(1)1.4g / INDOPACOM (b)(1)1.4a

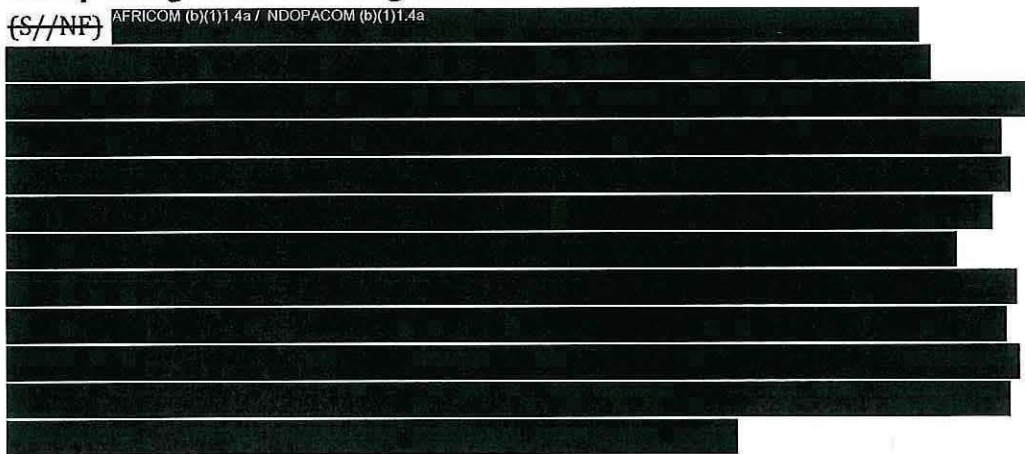
A large rectangular area of the document is completely redacted with black ink, covering approximately 12 lines of text.

(S) NDOPACOM (b)(1)1.4a

A rectangular area of the document is redacted with black ink, covering approximately 3 lines of text.

(U) Access to the Right Communication Tools Is Critical in Competing With Strategic Adversaries


(S//NF) AFRICOM (b)(1)1.4a / NDOPACOM (b)(1)1.4a

A large rectangular area of the document is redacted with black ink, covering approximately 12 lines of text.

(U) Management Comments on the Findings and Our Response

(U) USCENTCOM Comments to the Finding That USCENTCOM Regulation Authorized Use of Non-DoD-Controlled Electronic Messaging Systems Despite DoD Policy

(S) CENTCOM (b)(1)1.4a, (b)(1)1.4g / INDOPACOM (b)(1)1.4a

A rectangular area of the document is redacted with black ink, covering approximately 3 lines of text.

(S) CENTCOM (b)(1)1.4a, (b)(1)1.4g / INDOPACOM (b)(1)1.4a
[Redacted text block]

(S) CENTCOM (b)(1)1.4a, (b)(1)1.4g / NDOPACOM (b)(1)1.4a
[Redacted text block]

(S) CENTCOM (b)(1)1.4a, (b)(1)1.4g / NDOPACOM (b)(1)1.4a
[Redacted text block]

(U) Our Response

(S) CENTCOM (b)(1)1.4a, (b)(1)1.4g / NDOPACOM (b)(1)1.4a
[Redacted text block]

(S) CENTCOM (b)(1)1.4a, (b)(1)1.4g / NDOPACOM (b)(1)1.4a
[Redacted text block]

(S) CENTCOM (b)(1)1.4a, (b)(1)1.4g / NDOPACOM (b)(1)1.4a
[Redacted text block]

(S) CENTCOM (b)(1)1.4a, (b)(1)1.4g / NDOPACOM (b)(1)1.4a
[Redacted text block]

(U) USCENTCOM's comments show the importance of fully implementing all of our recommendations together. Recommendation 1 seeks to promote the needs of those working closely with foreign partners and their challenges when making enterprise policy and technology decisions. Recommendation 2 seeks to mitigate risk by strengthening OPSEC programs and training so that personnel are better aware of the risks they are accepting. Recommendation 3 seeks to tailor the use of DoDI 8170.01's exception criteria to reflect the operational conditions, threat environment, and commander's intent for each CCMD. In fact, CCR 380-8 already includes many of the elements of Recommendation 3. USCENTCOM's revision of CCR 380-8 to fully adopt DoDI 8170.01's requirements will strengthen OPSEC while providing commanders and personnel the flexibility they need to successfully conduct operations.

(U) Recommendations, Management Comments, and Our Response

(U) Recommendation 1

(U) We recommend that the Chief Information Officer for the Department of Defense, in coordination with the Under Secretary of Defense for Intelligence and Security, conduct a needs assessment to better understand the technological limitations of U.S. foreign partners and how they impact the combatant command's ability to communicate and collaborate with these partners. This assessment should inform recommendations for DoD enterprise technology solutions to improve communications interoperability with foreign partners.

(U) Office of the Chief Information Officer for the Department of Defense Management Comments

(U) The DoD Deputy CIO for Information Enterprise, on behalf of the DoD CIO, agreed with the recommendation. The DoD CIO, in coordination with the Secretary of the Air Force, the USD(I&S), and the Joint Staff J6 (through reporting by the DoD MPE Executive Steering Committee), will conduct a focused session with CCMDs and other select DoD Components to assess whether existing policy and processes effectively support the DoD's ability to communicate and collaborate with mission partners. This approach is consistent with the current awareness of the DoD CIO, Secretary of the Air Force, USD(I&S), and Joint Staff J6 regarding the technological shortcomings presented by the Department's mission partners as evidenced by existing and emerging communication and collaboration capabilities resulting from:

- (U) continuous CCMD and partner engagements;
- (U) the Joint Staff and Intelligence requirements processes; and
- (U) supporting governance and management forums.

(U) Our Response

(U) Comments from the DoD Deputy CIO for Information Enterprise met the intent of our recommendation. Therefore, the recommendation is resolved but will remain open. We will close this recommendation once the DoD CIO provides documentation from the focused session and we verify that the session addressed the findings of this report and developed a plan to implement the solutions.

(U) Recommendation 2

(U) We recommend that the Under Secretary of Defense for Intelligence and Security:

- a. **(U) Develop policy to strengthen the DoD operations security program and promote integration of operations security into future DoD operations and activities to mitigate the risks of using non-DoD-controlled electronic messaging systems; and**
- b. **(U) Develop operations security training requirements on the risks of sharing DoD information on non-DoD-controlled systems and add these requirements to the existing training requirements described in DoD Instruction 8170.01, "Online Information Management and Electronic Messaging," August 24, 2021, and DoD Directive, 5205.02E, "DoD Operations Security (OPSEC) Program," June 20, 2012, (Incorporating Change 2, August 20, 2020).**

(U) Under Secretary of Defense for Intelligence and Management Actions Taken

~~(CUI)~~ On November 10, 2021, we notified USD(I&S) personnel of our findings and recommendation that they should develop policy to mitigate the risks of using non-DoD-controlled electronic messaging systems and develop additional OPSEC training requirements on the risks of sharing DoD information on non-DoD-controlled systems.

~~(CUI)~~ The Chief of DoD OPSEC, responding on behalf of the USD(I&S), agreed with the recommendation. Specifically, the Chief of DoD OPSEC stated that the DoD CIO and the USD(I&S) are coordinating a draft memorandum, "Use of Non-Government Owned Mobile Devices," to establish minimum requirements for the use of non-government owned mobile devices to store, process, transmit, or display information up to DoD CUI. The scope is limited to mobile device information technology with mobile operating systems used to access and process up to DoD CUI, as defined in DoDI 5200.48 and Defense Information Systems Agency Cloud Computing Security Requirements Guide v1R3.

~~(CUI)~~ Additionally, the USD(I&S) plans to add a new question to the 2022 OPSEC data call to see if DoD Components proactively added additional training on the risk of sharing DoD information on non-DoD controlled systems in response to the June 2021 memo from the USD(I&S). Furthermore, the USD(I&S) plans to add a training requirement on using non-DoD systems and equipment as they update applicable DoD directives and manuals to specifically address the responsible and effective use of electronic messaging services and reference back to DoDI 8170.01.

(U) Our Response

(U) The USD(I&S) management actions taken prior to the issuance of the report met the intent of our recommendation. Therefore, the recommendation is resolved but will remain open. We will close the recommendation once we receive and review the signed memorandum, "Use of Non-Government Owned Mobile Devices;" the new (U) question added to the 2022 OPSEC data call; and the updated policies with the training requirement.

(U) Recommendation 3

(U) We recommend that the Commanders of the U.S. Africa Command, U.S. Central Command, U.S. European Command, U.S. Indo-Pacific Command, and U.S. Southern Command:

- a. (U) Issue command-level guidance clarifying the use of non-DoD-controlled electronic messaging systems. This guidance should include:
 - i. (U) any area of responsibility-specific conditions that permit personnel to use non-DoD-controlled messaging systems;
 - ii. (U) what information can be shared over the electronic messaging system;
 - iii. (U) how personnel are to maintain records generated on non-DoD systems in accordance with records management regulations;
 - iv. (U) how to report any security violations or misuse of a system;
 - v. (U) a process to ensure that any use of non-DoD-controlled electronic messaging systems meets the exception criteria in DoD Instruction 8170.01, "Online Information Management and Electronic Messaging," August 24, 2021;
 - vi. (U) additional training criteria for personnel that addresses the risks of using non-DoD electronic messaging systems, violating operations security regulations, and consequences of noncompliance; and
- b. (U) Establish risk assessment procedures to evaluate and monitor combatant command use of current and emerging information technologies to identify opportunities for use and to assess risks in accordance with DoD Instruction 8170.01, "Online Information Management and Electronic Messaging," August 24, 2021.

(U) USAFRICOM Management Actions Taken

(U) On November 18, 2021, we informed USAFRICOM of our findings and recommendation for USAFRICOM to develop command-level guidance on the use of non-DoD controlled electronic messaging systems and compliance with DoDI 8170.01. In response, the USAFRICOM Chief of Cybersecurity J62, responding on behalf of the USAFRICOM Commander, agreed with the recommendation and provided a plan of action to publish a USAFRICOM Instruction to address the recommendation along with milestones and the points of contact responsible.

(U) Our Response

(U) USAFRICOM management actions taken and plans provided before the issuance of our report met the intent of our recommendation. Therefore, the recommendation for USAFRICOM is resolved but remains open. We will close the recommendation once we receive and review documentation of the published USAFRICOM Instruction.

(U) USCENTCOM Management Comments

(U) The USCENTCOM Chief of the Cyber Security Division, responding on behalf of the USCENTCOM Commander, agreed with the recommendation and stated that USCENTCOM is revising CCR 380-8 and will adopt the guidance and develop subsequent training in accordance with DoDI 8170.01.

(U) Our Response

(U) Comments from the Chief of the Cyber Security Division met the intent of the recommendation. Therefore, the recommendation is resolved but will remain open. We will close the recommendation once we receive and review documentation of the updated CCR 380-8.

(U) USEUCOM Management Comments

(U) The USEUCOM J6 Director, responding on behalf of the USEUCOM Commander, agreed with the recommendation. The USEUCOM J6 Director stated that the USEUCOM J6 staff would update USEUCOM Command Instruction 6302.01A, "Internet-Based Capabilities Usage," to provide command-level guidance clarifying the use of non-DoD-controlled electronic messaging systems for official business. Additionally the USEUCOM J6 staff will update USEUCOM Command Instruction 6302.01A to establish risk assessment procedures to evaluate and monitor use of commercial information technologies in accordance with DoD Instruction 8170.01.

(U) Our Response

(U) Comments from the USEUCOM J6 Director met the intent of our recommendation. Therefore, the recommendation is resolved but will remain open. We will close the recommendation once we receive and review documentation of the updated USEUCOM Command Instruction 6302.01A.

(U) USSOUTHCOM Management Comments

(U) The USSOUTHCOM Command Inspector General, responding on behalf of the USSOUTHCOM Commander, agreed with the recommendation and stated that USSOUTHCOM Policy Letter 09-21, "Commercial Owned Electronic Messaging (U) Applications," meets many of the elements of the recommendation. The Inspector General stated that USSOUTHCOM would incorporate Recommendation 3.a.iv., 3.a.vi., and 3.b. in the next revision of Policy Letter 09-21 and use the current security procedures described in other USSOUTHCOM policies until the revision.

(U) Our Response

(U) Comments from the USSOUTHCOM Command Inspector General met the intent of our recommendation. Therefore, the recommendation is resolved but will remain open. We will close the recommendation once we receive and review the updated USSOUTHCOM Policy Letter 09-21.

(U) USINDOPACOM Management Comments Required

(U) The USINDOPACOM Commander did not respond to the recommendations in the report. Therefore, the recommendations are unresolved. We request that the Commander provide comments on the final report.

(U) Appendix

(U) Scope and Methodology

(U) We conducted this evaluation from June 2021 through February 2022 in accordance with the "Quality Standards for Inspections and Evaluations," published in December 2020 by the Council of the Inspectors General on Integrity and Efficiency. Those standards require that we plan and perform the evaluation to obtain sufficient and appropriate evidence to provide reasonable basis for our findings and conclusion based on our evaluation objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusion based on our evaluation objective.

(U) We obtained, reviewed, and analyzed the following DoD criteria:

- (U) DoDI 8170.01
- (U) DoDI 5015.02
- (U) DoDD 5205.02E

(U) The CCMDs included in this evaluation were USAFRICOM, USCENTCOM, USEUCOM, USINDOPACOM, and USSOUTHCOM. The Service component commands considered for this evaluation were:

- (U) USAFRICOM and USEUCOM:
 - (U) U.S. Army Europe and Africa (USAREURAF)
 - (U) U.S. Air Forces Africa
 - (U) U.S. Marine Corps Forces Africa
 - (U) U.S. Naval Forces Europe-Africa (NAVEUR-NAVAF)
- (U) USCENTCOM:
 - (U) U.S. Army Central (ARCENT)
 - (U) U.S. Naval Forces Central Command (NAVCENT)
 - (U) U.S. Air Forces Central Command (AFCENT)
 - (U) U.S. Marine Corps Forces Central Command (MARCENT)

- (U) USINDOPACOM:
 - (U) U.S. Pacific Fleet
 - (U) U.S. Pacific Air Forces
 - (U) U.S. Army Pacific
 - (U) U.S. Marine Forces Pacific
- (U) USSOUTHCOM:
 - (U) U.S. Army South (ARSOUTH)
 - (U) U.S. Air Forces Southern (AFSOUTH)
 - (U) U.S. Marine Corps Forces South (USMARFORSOUTH)
 - (U) U.S. Naval Forces Southern Command/4th Fleet (USNAVSO/FOURTHFLT)

(U) The evaluation also considered other component commands, such as the theater special operations commands and operation-specific commands, such as Combined Joint Task Force-Operation Inherent Resolve.

(U) To answer the evaluation objective, we interviewed personnel from the CCMDs and their component commands. We asked questions to help us better understand their roles and responsibilities; the tools they used to communicate with the foreign partners; the communication challenges they faced with foreign partners nations and how they mitigated those challenges during the COVID-19 pandemic; and how those mitigation strategies could be used in future operations where personal interaction is not possible.

(U) Additionally, we interviewed personnel from the Office of the Under Secretary of Defense for Intelligence and Security (USD(I&S)) and sent requests for information to the DoD Chief Information Officer (DoD CIO), the National Guard Bureau's State Partnership Program (NGB SPP), and the SAF/AA MPCO to understand how they provided support for foreign partner communications during the COVID-19 pandemic.

(U) We obtained, reviewed, and analyzed the following documentation to understand the impacts of the COVID-19 pandemic on communication operations, exercises, and mission-essential functions:

- (U) CCMD responses to our requests for information;
- (U) Command Campaign Plans for USAFRICOM, USCENTCOM, USEUCOM, USINDOPACOM, and USSOUTHCOM;
- (U) USCENTCOM FY21-25 Country Security Cooperation Plans;
- (U) The Joint Chiefs of Staff COVID-19 Military Response In-Stride Review Consolidated Report; and
- (U) Additional documents provided by the DoD CIO, USD(I&S), NGB SPP, and SAF/AA MPCO in response to our request for information.

(U) Management Comments

(U) DoD Chief Information Officer



CHIEF INFORMATION OFFICER

DEPARTMENT OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-6000

MEMORANDUM FOR INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE

SUBJECT: Review and Comment of DoD Inspector General "Evaluation of Combatant Commands' Communications Challenges with Partner Nations During the Corona Virus Disease-2019 Pandemic and Mitigation Efforts" (D2021-DEVOPD-0132.000) Draft Report

DoD IG RECOMMENDATION: The DoD Chief Information Officer (CIO), in coordination with the Undersecretary of Defense for Intelligence and Security (USD(I&S)), conduct a needs assessment to better understand the technological limitations of U.S. foreign partners and how they impact the combatant command's ability to communicate and collaborate with these partners. This assessment should inform recommendations for DoD enterprise technology solutions to improve communications interoperability with foreign partners.

DoD CIO RESPONSE: The DoD CIO supports the recommendation in the subject report. DoD CIO, in coordination with the Secretary of the Air Force (SECAF), USD(I&S), and the Joint Staff (JS) J6 through reporting by the 1-2 Star/SES chaired DoD Mission Partner Environment (MPE) Executive Steering Committee, will conduct a focused session with Combatant Commands and other select DoD Components to assess whether existing policy and processes effectively support Components' abilities to communicate and collaborate with mission partners. This approach is consistent with the current awareness of DoD CIO, SECAF, USD(I&S), and JS J6, regarding the technological shortcomings presented by the Department's mission partners as evidenced by existing and emerging communication and collaboration capabilities resulting from:

- Continuous Combatant Command and partner engagements;
- The Joint Staff and Intelligence requirements processes to include the DoD MPE Executive Agent's Unclassified Information Sharing Service Analysis of Alternatives; and
- Supporting governance/management forums (i.e., C4/Cyber Functional Capabilities Board, Digital Modernization Infrastructure Executive Committee, Defense Intelligence Information Environment Council, DoD MPE Senior Leader Board, DoD MPE ESC and its supporting working groups).

The point of contact for this matter is [DOD OIG (b)(6)] He can be reached at [DOD OIG (b)(6)] or [DOD OIG (b)(6)]@mail.mil.

METZ, DANIELLE. Digitally signed by METZ, DANIELLE
A, [DOD OIG (b)(6)] Date: 2022.02.16 11:32:55 -0500

Danielle A. Metz
Deputy Chief Information Officer for
Information Enterprise

~~SECRET/NOFORN~~

(U) United States Central Command



~~SECRET~~
UNCLASSIFIED WHEN SEPARATED FROM ATTACHMENTS

UNITED STATES CENTRAL COMMAND
7115 SOUTH BOUNDARY BOULEVARD
MACDILL AIR FORCE BASE, FLORIDA 33621-5101

15 February 2022

FROM: CCJ6-C

TO: CCIG/Audit

SUBJECT: DODIG D2021-DEV0PD-0132.000 Draft Report "Evaluation of Combatant Commands Communication Challenges with Foreign Nation Partners during COVID-19 Pandemic and Mitigation Efforts" (USCC-220203-QP746) (U)

1. (U) The USCENCOM CCJ6 has conducted a comprehensive review of the subject report and recommendations. USCENCOM CCJ6 partially concurs with the draft DODIG report. Our comments are attached as an enclosure.

2. (U) Thank you for the opportunity to review. We are available for any questions.

3. (U) POC for this action is CCJ6-C, Cybersecurity Division, at CENTCOM (b)(6) or at the following email: centcom.macdill.centcom-hq.mbx.ccj6-c@mail.smil.mil.

CENTCOM (b)(6)

CENTCOM (b)(6)

Encl:
CCJ6 Comment Narrative to CCIG 15 Feb 22 (S)

Classified By: CENTCOM (b)(6)
Derived From: USCENCOM SCG, CCR 380-14, 12 April 2021.
Declassify On: 2047-02-14

~~SECRET~~
UNCLASSIFIED WHEN SEPARATED FROM ATTACHMENTS

~~SECRET/NOFORN~~

United States Central Command (cont'd)

~~SECRET~~

DODIG D2021-DEVOPD-0132.000 Draft Report "Evaluation of Combatant Commands Communication Challenges with Foreign Nation Partners during COVID-19 Pandemic and Mitigation Efforts" (U)

Response to USCC 220203-OP746 TMT Tasker (16 February 2022):

(U) USCENTCOM "concur with comments" regarding DODIG D2021-DEVOPD-0132.000 Draft Report with attention to the following comments:

- (U) Concur with the Recommendations 3.a (i-vi) and 3.b. US Central Command CCR 380, *Cybersecurity and Support to Defensive Cyberspace Operations*, February 05, 2021, is currently under revision and will adopt the guidance (and develop subsequent training and awareness) established in DoD Instruction 8170.01, August 24, 2021. Estimated Completion date: 30 April 2022.

- (U) Comment / Change request: CENTCOM / INOPACOM (b)(1)1.7(e)



(U) Background/ Discussion:

CENTCOM (b)(1)1.4a, (b)(1)1.4g / INOPACOM (b)(1)1.4a

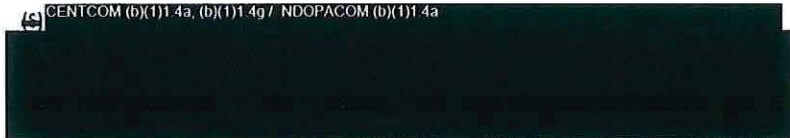


Classified By: CENTCOM (b)(6)
Derived From: USCENCOM SCG, CCR 380-14, 12 April 2021.
Declassify On: 2047-02-14


~~SECRET~~

United States Central Command (cont'd)

~~SECRET~~
(S) CENTCOM (b)(1)1.4a, (b)(1)1.4g / NDOPACOM (b)(1)1.4a



(S) CENTCOM (b)(1)1.4a, (b)(1)1.4g / NDOPACOM (b)(1)1.4a



(U) In order to find alternative solutions to meet operational needs while balancing OPSEC and Cybersecurity requirements, the CSISR conference included a cybersecurity track with focus on the threats, usage and impact of commercial encryption messaging applications as a communication tool for ground operations in the USCENTCOM Area of Responsibility (AOR). The challenges of records management, information-control and oversight, risks of exploitation, etc. were discussed. USCENTCOM sought out DoD-available solutions that would meet these requirements and identified a promising application, referred to as Wickr, that had been developed by the Air Force and was undergoing pilot testing with SOCOM (at the time). Wickr demonstrated the ability to prevent the dissemination of messages (e.g., forward, screenshot, print, etc.) and maintained positive control and audit of all transmissions; however, the subsequent discussion with partners and local nationals revealed that they would be unwilling to download/install any US military-developed solution and would only trust neutral, commercial applications. At that time, efforts to find alternative (potentially costly) technical solutions halted.

(U) Policy on Commercially Available Encrypted Messaging applications was drafted as USCENTCOM Policy Letter #108 but formally incorporated into the annual review of Central Command Regulation (CCR) 380-8, "Cybersecurity and Support to Defensive Cyberspace Operations", on 05 Feb 21, signed by USCENTCOM Chief of Staff. The objective of the language submitted in this policy was to reduce risks and limit the usage of these applications as a "last resort". If exceptions to policy were necessary to meet operational Commander requirements, it required operational justification; was intended to be temporary and include risk mitigation plans.

— Excerpt from CCR 380-80 (U)

4.3. USE OF COMMERCIAL APPLICATIONS FOR OFFICIAL COMMUNICATIONS

a. Use of Commercially-Available Encrypted Messaging (CAEM) applications for routine or official use of communications between DoD organizations, U.S. Government agencies and

United States Central Command (cont'd)

~~SECRET~~

partner nations can be utilized in the USCENTCOM AOR. The use of CAEM applications should only be used on U.S. Government furnished communication devices provided to U.S. personnel. Non U.S. personnel should only use non-government owned mobile devices. It is recommended non-government owned mobile devices and installed applications should only be used to communicate routine unclassified information.

b. Transmission of classified information to include photo and videos outside of secure DoD channels is prohibited. Sensitive or critical information must be transmitted by authorized secure means. Secure means includes DoD/U.S. government approved encrypted applications (e.g., Secret Internet Protocol Router Network).

c. Unauthorized installation of unapproved solutions to DoDIN-connected assets creates a system vulnerability. Only DoD-approved CAEM are authorized for installation on DoDIN connected assets. Any exploratory applications or pilot solutions under evaluation should be approved for U.S. government use.

d. Exception to this policy can be approved by the Service Component Commander or by the Joint Task Force Commander (e.g., U.S. Forces-Afghanistan or Combined Joint Task Force-Operation INHERENT RESOLVE). Each exception should contain the following information:

(1) Justification demonstrating an urgent operational need, specifying limited duration required.

(2) Risk Mitigation plan that includes the following:

(a) The CAEM software requested.

(b) Confirmation that the assets/equipment utilized will be U.S. government furnished equipment, not connected to DoDIN. Exceptions for the use of CAEM applications on personal communication devices such as cellular phones should be approved by Service Component Commander or by the Joint Task Force Commander.

(c) Description of appropriate measures to be taken to prevent exploitation and risk to mission; confirmation that application security management settings are configured to disable geolocation and active device management practices are established (e.g., backups and current software updates) pursuant to Reference (ppp).

(3) Data management and retrieval plans to ensure compliance with Reference (j)

e. Exceptions should only be authorized as a temporary solution and recommended be reevaluated semi-annually.

~~SECRET~~

(U) United States European Command



UNCLASSIFIED

UNITED STATES EUROPEAN COMMAND
UNIT 30400
APO AE 09131

ECJ6

15 February 2022

MEMORANDUM FOR Overseas Contingency Operations United States Department of
Defense Office of Inspector General

SUBJECT: (U) U.S. European Command (USEUCOM) Response to DoDIG Draft Report
Project No. D2021-DEVOPD-0132.000

References: (U) Draft Department of Defense Inspector General Report, *Evaluation of
Combatant Commands' Communication Challenges with Foreign Partner Nations During the
Coronavirus Disease-2019 Pandemic and Mitigation Efforts*, February 2, 2022 (S/NF)

1. (U) I concur with the Geographic Combatant Command recommendations within the report. Specifically, there were two items listed under "Recommendation 3" in the draft report. Implementation details are listed below.
2. (U) In accordance with Recommendation 3.a., the USEUCOM J6 staff will update USEUCOM Command Instruction (ECI) 6302.01A, *Internet-Based Capabilities Usage*, to provide command-level guidance clarifying the use of non-DoD-controlled electronic messaging systems for official business.
3. (U) Similarly, the USEUCOM J6 staff will update ECI 6302.01A to establish risk assessment procedures to evaluate and monitor use of commercial information technologies in accordance with DoD Instruction 8170.01.
4. (U) My point of contact for this matter is [REDACTED] EUCOM (b)(3), (b)(6)

[REDACTED]
EUCOM (b)(6)

CHAD D. RADUEGE
Brigadier General, U.S. Air Force
Director, C4/Cyber

UNCLASSIFIED

(U) United States Southern Command

UNCLASSIFIED



REPLY TO
ATTENTION OF

DEPARTMENT OF DEFENSE
UNITED STATES SOUTHERN COMMAND
9301 NW 33RD ST
DORAL, FL 33172-1217

SCPAO/SCIG

03 March 2022

MEMORANDUM FOR Department of Defense Office of Inspector General Overseas
Contingency Operations

SUBJECT: SOUTHCOM's response to the Evaluation of Combatant Command
Communication Challenges with Foreign Partner Nations during the COVID-19
Pandemic (Project No. D2021-DEVOPD-0132.000)

1. (U) Recommendation One: SOUTHCOM agrees and welcome an assessment by the Chief Information Officer for the Department of Defense, in coordination with the Under Secretary of Defense for Intelligence and Security, to better understand the technological limitations of U.S. foreign partners and how they impact combatant commands' ability to communicate and collaborate with our partners.

2. (U) Recommendation Two: SOUTHCOM's OPSEC lead in the J3 call the recommendation sound. Use of non-DoD-controlled electronic messaging systems and PEDs are already a point of emphasis for the SOUTHCOM Command OPSEC program. We will ensure that is highlighted as an increased item of interest for training and awareness through direct contact with our components, SCOs, JTFs, and within the HQ and Garrison. This will also be included as an action item for the SOUTHCOM Security Managers Working Group and addressed during ad hoc, periodic, and scheduled quarterly Working Group meetings.

The activities will be a continuous, consistent, and persistent effort pushed via our SOUTHCOM OPSEC Program (Program Managers at the HQ, Components, SCOs, and JTFs) and the aforementioned SOUTHCOM Security Managers Working Group (led by INFOSEC). Will confer with our SCJ6 for their actions/comments as well. Estimate completion date to integrate/emphasize these actions by end of 2nd quarter FY22 or NLT the first Security Managers meeting of 3rd quarter FY22.

3. (U) Recommendation Three: SOUTHCOM Policy 09-21, meets most of the draft recommendations, but there are some items that need to be addressed in an update. Meeting the recommendations will require the collaboration and involvement of multiple directorates [e.g. SCJ2 Security Management, SCJ3 (OPSEC and JCC/COIPE), SC-SJA,

UNCLASSIFIED

(U) United States Southern Command (cont'd)

UNCLASSIFIED

SCPAO/SCIG


SUBJECT: SOUTHCOM's response to the Evaluation of Combatant Command Communication Challenges with Foreign Partner Nations during the COVID-19 Pandemic (Project No. D2021-DEVOPD-0132.000)

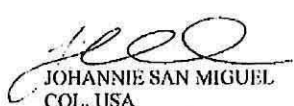
SC-KM/RM] in order to ensure we have a complete process that will be supported by our SC leadership.

Specifically, the rewrite of the SOUTHCOM Policy 09-21, will need to address:

- iv. (U) how to report any security violations or misuse of a system;
- vi. (U) additional training criteria for personnel that addresses the risks of using non-DoD electronic messaging systems, violating operations security regulations, and consequences of noncompliance; and
- b. (U) Establish risk assessment procedures to evaluate and monitor combatant command use of current and emerging information technologies to identify opportunities for use and to assess risks in accordance with DoD Instruction 8170.01, "Online Information Management and Electronic Messaging," August 4, 2021.
- 4. (U) Incorporating recommendations "iv", "vi", and "b" from the draft report is not to say, the SOUTHCOM Enterprise lacks a system to report security violations and/or misuse of a system or protocols to retrain personnel when violations are made. A system to do this is in place at SOUTHCOM, this is just not captured in the SC Policy 09-21. Additionally, in our SC Enterprise Network Request system when new, current, or emerging IT hardware and software is requested, risk assessments are conducted and reviewed prior to procurement. This process can also be amplified in the SC Policy.

5. (U) The point of contact for this memo is [REDACTED] at [REDACTED] email [REDACTED] @mail.smil.mil or [REDACTED] at [REDACTED] email [REDACTED] @mail.smil.mil.


EMANUELE ORTIZ
COL, USA
Public Affairs Chief


JOHANNIE SAN MIGUEL
COL, USA
Inspector General

UNCLASSIFIED

(U) Sources of Classified Information

(U) **Source 1:** (U) United States European Command CDRUSEUCOM Combatant Command Campaign Plan 2020 (November 2020) (SECRET//NOFORN)
Declassification Date: December 31, 2045
Date of Source: November 2020

(U) **Source 2:** (U) U.S. Indo-Pacific Command Campaign Plan (July 1, 2020) (SECRET//REL TO USA, FVEY)
Declassification Date: July 1, 2045
Date of Source: July 1, 2020

(U) **Source 3:** (U) United States Southern Command Campaign Plan 6000-20 Change 1 Fiscal Years 2020-2024 (April 1, 2021) (SECRET//NOFORN)
Declassification Date: April 1, 2046
Date of Source: April 1, 2021

(U) **Source 4:** (U) U.S. Central Command Campaign Plan 1000-21 (February 25, 2021) (SECRET//REL TO USA, FVEY)
Declassification Date: January 22, 2031
Date of Source: February 25, 2021

(U) **Source 5:** (U) Appendix 19 to Annex C to USCENTCOM Campaign Plan 2021 (December 15, 2020) (SECRET//REL TO USA, FVEY)
Declassification Date: September 30, 2030
Date of Source: September 30, 2020

(U) **Source 6:** (U) United States Africa Command Campaign Plan 2000-21 (February 18, 2021) (SECRET//REL TO USA, FVEY)
Declassification Date: February 17, 2046
Date of Source: February 18, 2021

(U) **Source 7:** (U) Joint Chiefs of Staff COVID-19 Military Response In-Stride Review Consolidated Report (August 26, 2020) (SECRET//NOFORN)
Declassification Date: August 26, 2045
Date of Source: August 26, 2020

(U) **Source 8:** (U) U.S. Central Command FY21-25 Country Security Cooperation Plan for Iraq (September 30, 2020) (SECRET//REL TO USA, FVEY)
Declassification Date: September 30, 2030
Date of Source: September 30, 2020

(U) **Source 9:** (U) U.S. Central Command FY21-25 Country Security Cooperation Plan for Egypt (September 30, 2020) (SECRET//REL TO USA, FVEY)

Declassification Date: September 30, 2030

Date of Source: September 30, 2020

(U) **Source 10:** (U) U.S. Central Command FY21-25 Country Security Cooperation Plan for Bahrain (September 30, 2020) (SECRET//REL TO USA, FVEY)

Declassification Date: September 30, 2030

Date of Source: September 30, 2020

(U) **Source 11:** (U) U.S. Central Command FY21-25 Country Security Cooperation Plan for Arab Republic of the Emirates (September 30, 2020) (SECRET//REL TO USA, FVEY)

Declassification Date: September 30, 2030

Date of Source: September 30, 2020

(U) **Source 12:** (U) U.S. Central Command FY21-25 Country Security Cooperation Plan for Kazakhstan (September 30, 2020) (SECRET//REL TO USA, FVEY)

Declassification Date: September 30, 2030

Date of Source: September 30, 2020

(U) **Source 13:** (U) U.S. Central Command FY21-25 Country Security Cooperation Plan for Jordan (September 30, 2020) (SECRET//REL TO USA, FVEY)

Declassification Date: September 30, 2030

Date of Source: September 30, 2020

(U) **Source 14:** (U) U.S. Central Command FY21-25 Country Security Cooperation Plan for Lebanon (September 30, 2020) (SECRET//REL TO USA, FVEY)

Declassification Date: September 30, 2030

Date of Source: September 30, 2020

(U) **Source 15:** (U) U.S. Central Command FY21-25 Country Security Cooperation Plan for Kuwait (September 30, 2020) (SECRET//REL TO USA, FVEY)

Declassification Date: September 30, 2030

Date of Source: September 30, 2020

(U) **Source 16:** (U) U.S. Central Command FY21-25 Country Security Cooperation Plan for The Kyrgyz Republic (September 30, 2020) (SECRET//REL TO USA, FVEY)

Declassification Date: September 30, 2030

Date of Source: September 30, 2020

(U) **Source 17:** (U) U.S. Central Command FY21-25 Country Security Cooperation Plan for Qatar (September 30, 2020) (SECRET//REL TO USA, FVEY)

Declassification Date: September 30, 2030
Date of Source: September 30, 2020

(U) **Source 18:** (U) U.S. Central Command FY21-25 Country Security Cooperation Plan for Pakistan (September 30, 2020) (SECRET//REL TO USA, FVEY)
Declassification Date: September 30, 2030
Date of Source: September 30, 2020

(U) **Source 19:** (U) U.S. Central Command FY21-25 Country Security Cooperation Plan for Oman (September 30, 2020) (SECRET//REL TO USA, FVEY)
Declassification Date: September 30, 2030
Date of Source: September 30, 2020

(U) **Source 20:** (U) U.S. Central Command FY21-25 Country Security Cooperation Plan for Uzbekistan (September 30, 2020) (SECRET//REL TO USA, FVEY)
Declassification Date: September 30, 2030
Date of Source: September 30, 2020

(U) **Source 21:** (U) U.S. Central Command FY21-25 Country Security Cooperation Plan for Turkmenistan (September 30, 2020) (SECRET//REL TO USA, FVEY)
Declassification Date: September 30, 2030
Date of Source: September 30, 2020

(U) **Source 22:** (U) U.S. Central Command FY21-25 Country Security Cooperation Plan for Tajikistan (September 30, 2020) (SECRET//REL TO USA, FVEY)
Declassification Date: September 30, 2030
Date of Source: September 30, 2020

(U) **Source 23:** (U) U.S. Central Command FY21-25 Country Security Cooperation Plan for Saudi Arabia (September 30, 2020) (SECRET//REL TO USA, FVEY)
Declassification Date: September 30, 2030
Date of Source: September 30, 2020

(U) **Source 24:** (U) U.S. Central Command FY21-25 Country Security Cooperation Plan for Yemen (September 30, 2020) (SECRET//REL TO USA, FVEY)
Declassification Date: September 30, 2030
Date of Source: September 30, 2020

(U) **Source 25:** (U) U.S. Central Command FY21-25 Country Security Cooperation Plan for Afghanistan (September 30, 2020) (SECRET//REL TO USA, FVEY)
Declassification Date: September 30, 2030
Date of Source: September 30, 2020

~~SECRET/NOFORN~~

(U) **Source 26:** (U) Evaluation of the U.S. Africa Command's Response to Coronavirus Disease-2019 (September 30, 2020) (SECRET//NOFORN)

Declassification Date: June 4, 2045

Date of Source: September 30, 2020

(U) **Source 27:** (U) Evaluation of the U.S. Central Command's Response to Coronavirus Disease-2019 (March 3, 2021) (SECRET//NOFORN)

Declassification Date: July 31, 2045

Date of Source: March 3, 2021

(U) **Source 28:** (U) Evaluation of the U.S. European Command's Response to Coronavirus Disease-2019 (October 8, 2020) (SECRET//NOFORN)

Declassification Date: May 25, 2045

Date of Source: October 8, 2020

(U) **Source 29:** (U) Evaluation of the U.S. Indo-Pacific Command's Response to Coronavirus Disease-2019 (March 31, 2021) (SECRET//REL TO USA, FVEY)

Declassification Date: March 31, 2046

Date of Source: March 31, 2021

(U) **Source 30:** (U) Evaluation of the U.S. Southern Command's Response to Coronavirus Disease-2019 (March 31, 2021) (SECRET//NOFORN)

Declassification Date: March 26, 2044

Date of Source: March 31, 2021

~~SECRET/NOFORN~~

(U) Acronyms and Abbreviations

AOR	Area of Responsibility
CCMD	Combatant Command
CCR	Central Command Regulation
CIO	Chief Information Officer
CUI	Controlled Unclassified Information
CVR	Commercial Virtual Remote
COVID-19	Coronavirus Disease—2019
MPCO	Definition Mission Partner Capability Office
MPE	Mission Partner Environment
NGB	National Guard Bureau
OPSEC	Operations Security
PN	Partner Nation
SAF/AA	Secretary of the Air Force, Administrative Assistant
SPP	State Partnership Program
USD(I&S)	Under Secretary of Defense for Intelligence and Security
USAFRICOM	U.S. Africa Command
USCENTCOM	U.S. Central Command
USEUCOM	U.S. European Command
USINDOPACOM	U.S. Indo-Pacific Command
USSOUTHCOM	U.S. Southern Command

~~SECRET//NOFORN~~

Whistleblower Protection

U.S. DEPARTMENT OF DEFENSE

Whistleblower Protection safeguards DoD employees against retaliation for protected disclosures that expose possible fraud, waste, and abuse in Government programs. For more information, please visit the Whistleblower webpage at <http://www.dodig.mil/Components/Administrative-Investigations/Whistleblower-Reprisal-Investigations/Whistleblower-Reprisal/> or contact the Whistleblower Protection Coordinator at Whistleblowerprotectioncoordinator@dodig.mil

**For more information about DoD OIG
reports or activities, please contact us:**

Congressional Liaison
703.604.8324

Media Contact
public.affairs@dodig.mil; 703.604.8324

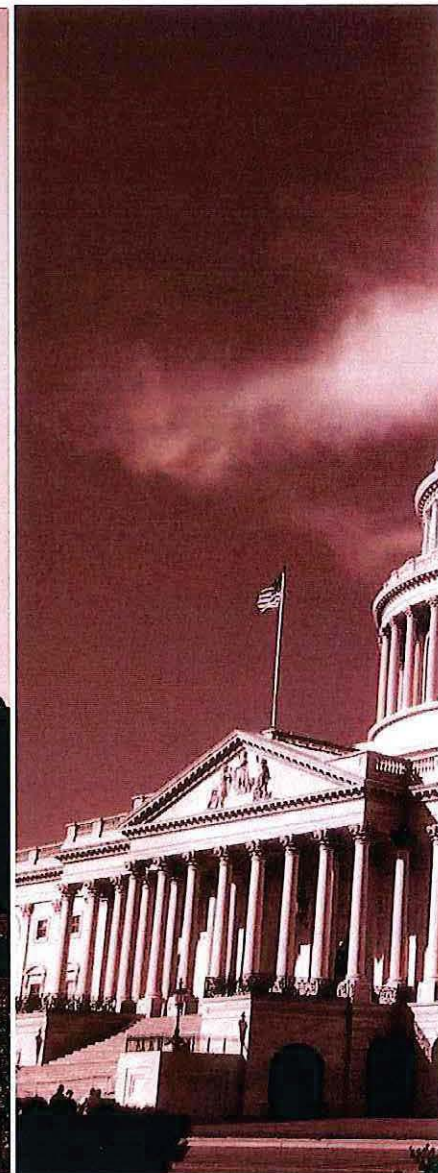
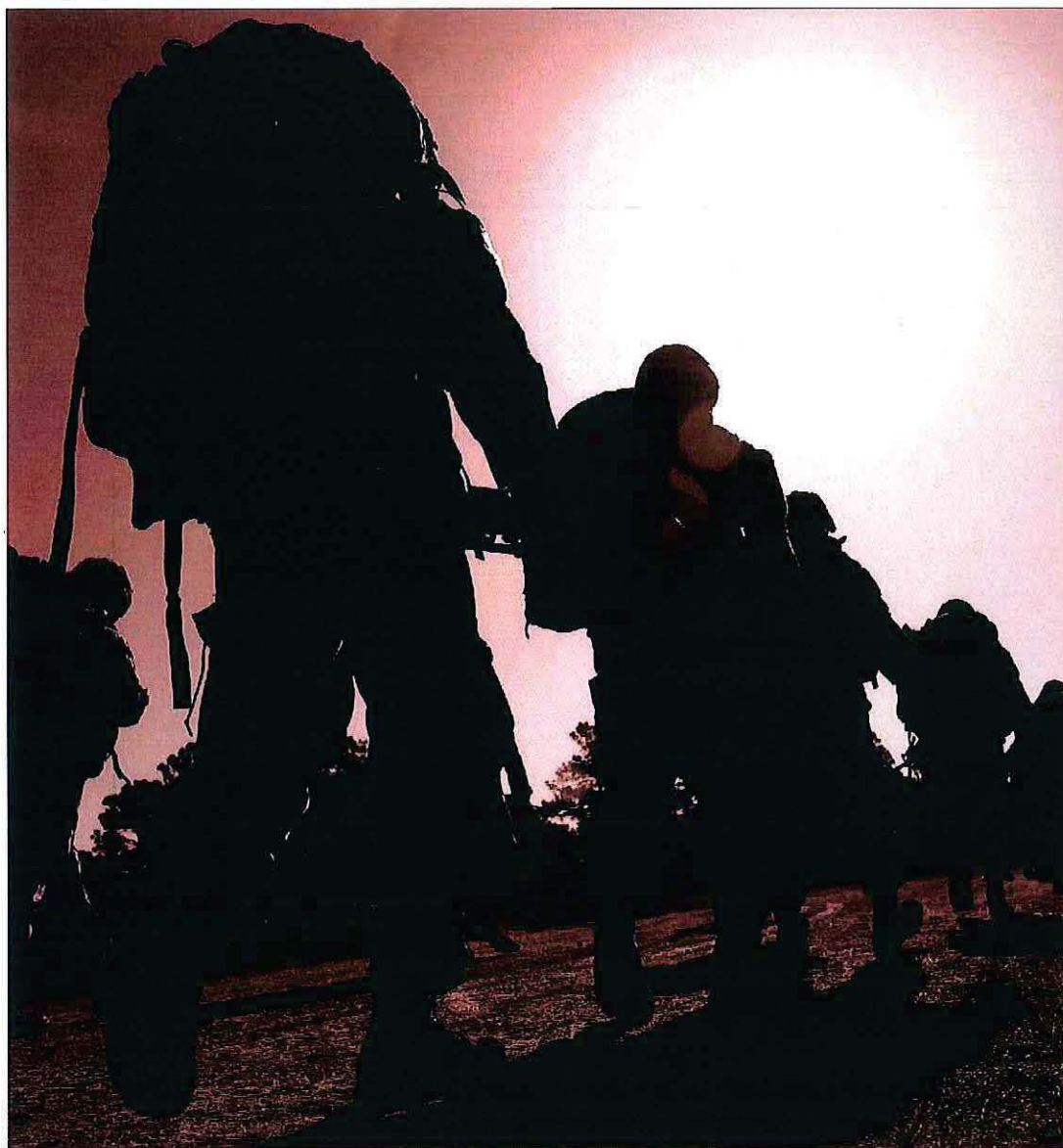
DoD OIG Mailing Lists
[www.dodig.mil/Mailing Lists/](http://www.dodig.mil/Mailing%20Lists/)

Twitter
www.twitter.com/DoD_IG

DoD Hotline
www.dodig.mil/hotline

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~



DEPARTMENT OF DEFENSE | OFFICE OF INSPECTOR GENERAL

4800 Mark Center Drive
Alexandria, Virginia 22350-1500
www.dodig.mil
DoD Hotline 1.800.424.9098

~~SECRET//NOFORN~~