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

CHIEF INFORMATION OFFICER

August 20, 2018

MEMORANDUM FOR: SEE DISTRIBUTION

SUBJECT: Interim Digital Authentication Guidelines for Unclassified and Secret Classified DoD Networks and Information Systems

References: (a) DoD Instruction 8520.02, "PKI and Public Key Enabling," May 24, 2011
(b) DoD Instruction 8520.03, "Identity Authentication for Information Systems," May 13, 2011, as amended

This memorandum provides interim guidance and clarification to the current policies for Department of Defense (DOD) Public Key Infrastructure (PKI) and identity authentication for privileged and authorized user-authentication. The DoD Chief Information Officer (CIO) issues and will incorporate the guidance provided herein to future revisions of references (a) and (b).

There are four (4) attachments to this memo with each attachment clarifying authentication requirements for the DoD. The attachments are:

- Attachment 1, DoD-approved Authentication Solutions, is a list of currently approved DoD Public Key Infrastructure (PKI), Multi-Factor Authentication (MFA), and Identity Federation Services (IFS) solutions.

- Attachment 2, DoD Approval Process for MFA and IFS Solutions, defines the required approval process for all DoD organizations to use when requesting use of an MFA or IFS solution not previously approved and listed in Attachment 1.

- Attachment 3, IFS Implementation Guidelines, lists the requirements for implementing an IFS solution on the Non-Secure Internet Protocol Router Network (NIPRNet) and the Secret Internet Protocol Router Network (SIPRNet).

- Attachment 4, DoD-approved Username/Password (UN/PW) Use Cases.

The points of contact for this memorandum are Colonel Tom Clancy, (571) 372-4594, thomas.j.clancy2.mil@mail.mil, and Mr. Charles "Andy" Seymour, (571) 372-6990, charles.a.seymour.civ@mail.mil.

Essye B Miller
Essye B. Miller
Principal Deputy

Attachments:
As stated

DISTRIBUTION:
Secretaries of the Military Departments
Chairman of the Joint Chiefs of Staff
Under Secretaries of Defense
Chief Management Officer
Chiefs of the Military Services
Chief, National Guard Bureau
Commandant of the Coast Guard
Commanders of the Combatant Commands
General Counsel of the Department of Defense
Director of Cost Assessment and Program Evaluation
Inspector General of the Department of Defense
Director of Operational Test and Evaluation
Assistant Secretary of Defense for Legislative Affairs
Assistant to the Secretary of Defense for Public Affairs
Director of NET Assessment
Director, Strategic Capabilities Office
Directors of the Defense Agencies
Directors of the DoD Field Activities

Attachment 1: DoD-Approved Authentication Solutions

DoD requires authorized users to authenticate to DoD information systems (IS) and applications with DoD-approved PKI credentials, but permits other DoD-approved authentication solutions when PKI is infeasible. DoD-approved Multi-Factor Authentication (MFA) or Identity Federation Service (IFS) solutions shall be considered before any other MFA or IFS solutions are considered. Capabilities not currently approved shall be reviewed by the Privilege User Working Group (PUWG). The PUWG and DoD Deputy CIO for Cybersecurity (DCIO-CS) will continue to evaluate other MFA and IFS capabilities for approval. Requirements for new systems should specify the use of DoD PKI. If PKI authentication cannot be implemented in a new system, then System Owners (SOs) must receive their Authorizing Official's (AO) approval for use of a DoD-approved interim MFA or IFS solution prior to contract award.

DoD privileged-users must comply with U.S. CYBERCOM TASKORD 14-0018, regardless of which DoD-approved authentication solution they use, except in instances where device administrators need limited access to web browsers in order retrieve PKI certificates for DoD devices from the DoD PKI Non-Person Entity (NPE) system.

I. **DoD-Approved PKI:** The following provides DoD approved authentication capabilities for DoD Unclassified and Secret networks.

   A. Unclassified Networks (e.g. Non-classified Internet Protocol Router Network (NIPRNet).

      1. Common Access Card (CAC). The CAC is the primary DoD PKI credential for logical authentication to unclassified DoD networks, systems, servers, and applications. The CAC meets the criteria for Authenticator Assurance Level (AAL) 3 in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63-3, "Digital Identity Guidelines."

      2. NIPRNet Alternate Logon Token (ALT). The DoD ALT is the mandated DoD PKI credential for authentication to privileged user accounts on the NIPRNet. The ALT is also used for group and role accounts, and may be used for NIPRNet logon in accordance with DoD Policy.

      3. External Certificate Authority (ECA) PKI Credentials. ECAs medium token assurance and medium hardware assurance PKI credentials may be used to authenticate to unclassified DoD IS, but may not be used for network logon and authentication to privileged-user accounts. These ECA PKI credentials meet the requirements for AAL3 in NIST SP 800-63-3. For more ECA information, see https://iase.disa.mil/pki/eca/Pages/index.aspx.

      4. Personal Identity Verification (PIV) PKI Credentials. DoD-approved Federal PIV PKI credentials qualify as AAL3. DoD-approved PIV PKI credentials may be used for both network logon and authentication to unclassified DoD IS on unclassified DoD networks. DoD-approved PIVs are listed at https://iase.disa.mil/pki-pke/interoperability/Pages/index.aspx.

5. PIV-Interoperable (PIV-I) and Industry Partner PKI Credentials. DoD-approved PIV-I PKI credentials and industry-partner medium hardware PKI credentials qualify as AAL3 in NIST SP 800-63-3. DoD-approved PIV-I PKI credentials and industry-partner medium hardware PKI credentials may be used to authenticate to unclassified DoD IS, but may not be used for network logon and authentication to privileged-user accounts. DoD-approved PIV-I PKI credentials and industry-partner medium-hardware PKI credentials are listed at: https://iase.disa.mil/pki-pke/interoperability/Pages/index.aspx.

6. Five-Eyes (FVEY) Mission Partner PKI Credentials. FVEY users must use either ECA Medium Token Assurance (or above) PKI credentials or their own unclassified PKI credentials to authenticate to unclassified DoD systems. Unclassified FVEY PKI credentials must be issued under a FVEY unclassified PKI Root Certificate Authority (CA) cross-certified with a DoD PKI, in line with Allied Communication Publication 185.

B. Secret Classified Networks (e.g. Secure Internet Protocol Router Network (SIPRNet).

1. National Security Systems (NSS) SIPRNet PKI Token. The NSS SIPRNet PKI Token is the primary credential for logical authentication to Secret classified DoD networks, systems, and applications.

2. DoD NSS SIPRNet PKI Admin-I token. The DoD NSS SIPR PKI Admin-I token is the mandated DoD PKI credential for authentication to DoD administrative accounts on the SIPRNet.

3. Federal Partners. NSS PKI tokens from other federal departments and agencies are approved for authentication to SIPRNet DoD resources, provided the federal entity has connected their NSS Secret classified network to the SIPRNet via the Federal Demilitarized Zone (FED DMZ) in accordance with the DoD CIO Memorandum, “Improving Security of Federal Department and Agency Connections to the DoD SIPRNet FED DMZ.”

4. Contractors at Contractor Facilities. DoD Contractors who access the SIPRNet via contractor-facility enclaves must obtain NSS SIPRNet PKI tokens from their DoD Component sponsors.

5. FVEY Mission Partner PKI Credentials on the SIPRNet. See attachment 4.

C. Mobile PKI credentials. At this time, DISA’s Purebred is the only authorized DoD Derived PKI credential issuance system. DoD-approved MFA and IFS may be used to authenticate to unclassified DoD resources via a mobile device.

II. **DoD-Approved Alternative (i.e. non-PKI) MFA and IFS:** SOs must implement MFA and IFS solutions in line with the guidance in their respective authorizing memos and applicable DISA guidance. MFAs must meet the requirements for IAL2/AAL2 in NIST SP 800-63-3, and IFS must meet the requirements in Attachment 3 of this memorandum. SOs must only implement current, fully patched versions of approved MFA device or IFS. AOs must approve the use of the specific DoD-approved MFA or IFS for a specific system or application. FVEY and other foreign mission partners may not utilize DoD-approved MFA or IFS to authenticate to IS on classified DoD networks, regardless of which IS or network the MFA or IFS is approved for. For more information on approved MFA and IFS, see the "DoD CIO Documentation" section at https://iase.disa.mil/idam/Pages/documentation.aspx.

A. DoD-approved MFA. MFA may only be used when either a system or application does not support authentication using DoD-approved PKI credentials, or a portion of the system or application's subscribers are unable to obtain DoD approved PKI credentials. The currently approved MFAs are:

1. RSA SecurID token. Approved for both unclassified and Secret classified DoD IS.

2. YubiKey Universal Two Factor token. Approved for both unclassified and Secret classified DoD IS.

3. SafeNet eToken PASS Model 3000. Approved for NIPRNet DoD IS.

B. DoD-approved IFS. IFS are third-party intermediary services (e.g. gateways, jump-boxes, F5 servers) facilitating user-authentication to resources or relying parties. IFS may only be used when a system or application does not support direct authentication with DoD approved PKI or MFA credentials, or the SO desires a single management framework for a group of heterogeneous systems. The currently approved IFS are:

1. Enterprise Privileged User Authentication Service (EPUAS). Approved for both unclassified and Secret classified DoD IS.

2. Secure Administration Authentication Gateway (SAAG). Approved for both unclassified and Secret classified DoD IS.

3. Centrify Server Suite (CSS) and Centrify Privileged Service (CPS). Approved for DoD IS on both the NIPRNet and SIPRNet.

4. United States Coast Guard (USCG) Remote Desktop Services (RDS) Jumpbox Solution. Approved for unclassified DoD IS.

III. DoD-approved Usernames (UN) and Passwords (PW):

A. DoD Self-service Logon (DS-Logon). DS-Logon is a secure, self-service logon ID account for unclassified DoD IS provided by the Defense Manpower Data Center (DMDC). DMDC is working to incorporate MFA options into DS-Logon.

B. Non-DS-Logon UN/PW. DoD Components may only issue non-DS-Logon UN/PWs for the use-cases described in Attachment 4. These UN/PWs must meet the requirements for IAL2/AAL1 in NIST SP 800-63-3. The UN/PW standards in reference (b) are no longer mandatory.

Attachment 2: DoD Approval Process for MFA and IFS Solutions

SOs seeking approval for MFA and IFS solutions that are not DoD-approved, should coordinate directly with their Component PKI Office during requirements identification and solution selection, and should only leverage the PUWG for its knowledge base. SOs must obtain approval of the proposed MFA/IFS solution from their DoD Component Chief Information Security Officer (CISO) before briefing the PUWG and seeking approval from the DCIO-CS. Contact information for many Component PKI Offices is at https://iase.disa.mil/pki-pke/Pages/contact.aspx. The PUWG Secretariat can be contacted directly at OSD.DoDCIO.PKI.Compliance@mail.mil.

I. The approval process begins when a DoD SO or AO for an unclassified or secret classified system submits a request for approval of an MFA or IFS solution to their Component CISO. The format of the MFA or IFS request should be in line with individual DoD Component rules and requirements. At a minimum, the substance of the request must include:

A. Why existing DoD-approved PKI, MFA, and IFS solutions cannot support the SO's needs. DoD-approved MFA and IFS solutions must be considered before any other MFA or IFS solutions are considered.

B. A detailed description of how the solution works.

C. Pilot/test results on the security and efficacy of the solution.

D. An assessment of the risks associated with approving the MFA or IFS solution for the DoD enterprise. At a minimum, the risk assessment must include sensitivity of the information on the system per reference (b), system vulnerabilities and the likelihood and impact of a system compromise, risk mitigations, and residual risk after implementing the mitigations.

E. Whether the MFA/IFS or MFA/IFS components are validated or under a National Information Assurance Partnership (NIAP) Protection Profile. The requester must provide evidence of validation.

F. Whether and how the MFA/IFS vendor is partially or wholly foreign-owned.

II. If the Component CISO deems implementation of the new MFA or IFS solution to be secure and effective, they may sign a written approval of the MFA or IFS solution. The SO/AO then contacts the PUWG Secretariat, and provides them the documentation submitted to their CISO and the CISO's written endorsement. To be considered for approval, the MFA or IFS solutions must at a minimum:

A. Meet the requirements for IAL2 and AAL2 (applies to MFA).

B. Comply with Attachment 3 of this Memorandum (applies only to IFS).

C. Require users to be individually authenticated.

D. Be the most current, fully-patched versions of the MFA or IFS.

E. Ensure credentials are not exposed in an environment that represents a high risk of compromise or hijacking, especially if they are used for privileged accounts.

F. Ensure access mechanisms resist replay of credentials.

III. The PUWG Secretariat confirms submission of a complete package of artifacts, and notifies the Cybersecurity Scorecard Team that a DoD Component CISO submitted a signed and complete package for an MFA or IFS solution. The Cybersecurity Scorecard Team then designates the Component user-accounts utilizing the MFA or IFS solution as compliant with Scorecard authentication requirements for the next 120 days, and notifies the Component CISO of this 120-day approval period.

A. The DoD CIO Identity and Access Management (IdAM)/PKI Lead may extend this approval period beyond 120 days if they determine the evaluation process requires more time.

IV. The PUWG Secretariat arranges for the SO/AO to brief the PUWG on the solution at the earliest possible date. After briefing the PUWG, the SO/AO has two weeks to respond to follow-up questions and engage in additional assessments or actions to resolve the concerns of PUWG members. After the SO/AO answers all questions to the PUWG's satisfaction, the DoD CIO IdAM/PKI Lead provides a recommendation to the DCIO-CS.

V. If, for whatever reason, the DoD CIO IdAM/PKI Lead does not make a recommendation of approval to the DCIO-CS, or the DCIO-CS chooses not to grant approval within the 120-day approval period (or when all extensions run out), the solution will be documented as disapproved and Cybersecurity Scorecard metrics will be adjusted accordingly going forward. Component AOs/SOs who requested the capability should seek to implement one of the DoD-approved PKI, MFA, or IFS solutions in Attachment 1 of this memorandum.

VI. If the DCIO-CS approves the MFA or IFS solution, the PUWG Secretariat will notify the DoD Cybersecurity Scorecard team of the approval, and ensure the approval memorandum is added to the DoD-approved MFA and IFS solution list at: https://iase.disa.mil/idam/Pages/documentation.aspx. The DCIO-CS may approve solutions for unclassified and/or Secret classified DoD networks, either as an enterprise solution or for an individual system or application. In addition, the DCIO-CS will.

A. Include basic implementation guidance in the approval memorandum, such as a requirement to use current, fully patched versions of the products in question. DoD Components must implement the approved MFA/IFS in line with all of the implementation guidance in the approval memo (in addition to applicable implementation guidance in this memorandum, such as Attachment 3 for IFS).

B. Include POC information in the approval memorandums for the SO or AO that brought the solution to the PUWG's attention.

C. Work with DISA to develop more extensive implementation guidance for approved MFA and IFS. Once DISA implementation guidance is published, SOs must configure all implementations of the MFA/IFS in line with DISA guidance.

D. Instruct the Cybersecurity Scorecard Team to evaluate the individual system or application for which the solution was requested as compliant with the pertinent PKI requirements, upon confirming proper implementation. If a solution was approved for the enterprise, then any system or application that implements it properly and within the parameters of the memo will be considered compliant.

VII. The system's AO shall re-evaluate its authorization of the MFA or IFS solution on an annual basis. The AO shall also ensure there is a Plan of Action and Milestones (POA&M) for replacing the MFA or IFS with DoD-approved PKI when PKI implementation becomes technically feasible and /or the system's subscribers are able to obtain DoD-approved PKI.

Attachment 3: Identity Federation Service (IFS) Implementation Guidelines

In order to obtain and maintain DoD-approval, DoD SOs must ensure, and their AOs must certify, that IFS devices and/or services are, at a minimum, configured to:

I. Require IAL2/AAL2 DoD-approved PKI or MFA credentials for the initial (e.g. front-end) authentication to the IFS, and convey this information about the initial user-authentication to the relying parties (i.e. the servers or applications behind the IFS). If users utilize PKI certificates, ensure certificate validation is implemented.

II. Require any system that passes authenticators outside of a system boundary to meet the criteria for Federated Assurance Level (FAL) 2.

III. Protect all web-traffic between the IFS and relying parties (including legacy systems) with secure applications to protect information from disclosure. Secure applications include, but are not limited to: Transportation Layer Security (TLS), Virtual Private Network (VPN) encrypted tunnels, Internet Protocol Security (IPsec), PuTTY sessions, Pageant, and Secure Shell (SSH).

IV. Block users from accessing the servers, systems, and applications behind the IFS without going through the IFS, except for a direct console connection after retrieving a password from the IFS. This could be done with non-routable Internet Protocols (IP) addresses, unique temporary passwords for each user-device session, or other technologies.

V. Block users from authenticating directly from one webserver or application behind the IFS to any other server, system, or application.

VI. Log every time a user accesses a server, system, or application via the IFS.

A. Generate audit records of successful and unsuccessful logon attempts.

B. Provide local session logging to a central location, which must capture, record, and log all content related to a user session.

VII. Require all privileged users administering and/or utilizing the IFS to operate in compliance U.S. CYBERCOM TASKORDER 14-0018, except in instances where device administrators need limited access to web browsers in order retrieve PKI certificates for DoD devices from the DoD PKI Non-Person Entity (NPE) system. When possible, IFS should utilize an Out of Band (OOB) capability for privileged users.

Attachment 4: DoD-approved Username/Password (UN/PW) Use Cases

The following use-cases describe situations and environments where DoD Components may issue DoD-approved (i.e. IAL2/AAL1) UN/PWs to users. DoD Components must implement risk mitigations for these use-cases to prevent users from accessing high-sensitivity information not essential to their mission. Reference (b) defines information sensitivity levels. DoD Component CISOs must validate, in Defense Cyberscope (DCS), all claims a network, IS or user(s) fall under one of these use-cases. DoD Components must utilize the DoD Risk Management Framework (RMF) described in DoDI 8510.01 to regularly verify whether username/password for the network, IS or user is still required. If an IS has both UN/PW users and non-UN/PW users, the IS must still require the non-UN/PW users to authenticate with DoD-approved PKI, MFA, or IFS.

I. **Unclassified DoD IS Residing on Unclassified DoD Networks**. For these use-cases, privileged users must authenticate with ALTs or DoD-approved MFAs.

A. Service members for life, dependents, and students. DoD retirees, dependents, students, and employees may authenticate from their own non-DoD personal devices to their Sensitivity Level 1 Personal Identity Information (PII) and Protected Health Information (PHI) with a DS-Logon UN/PW.

B. Nontraditional-Mission Systems. Users may authenticate with a DoD-approved non-DS Logon UN/PW to unclassified internet-based systems specifically intended to engage DoD mission partners, known and unknown, in nontraditional missions such as humanitarian assistance, disaster response, stability operations, or building partner capacity (e.g. Coalition Accounts, All Partners Access Network).

C. Non-FVEY Foreign Nationals. Non-FVEY Foreign Nationals authenticating from foreign countries who are not eligible for or cannot obtain CACs, ECAs, ALTs, or DoD-approved MFA, may authenticate with a DoD-approved non-DS Logon UN/PW to Sensitivity Level 1 and 2 information. DoD Components must closely monitor the activity of these users, and revoke, reissue, or reproof for passwords as necessary.

D. Pre-accession Recruits, Reservists, and National Guard members. Reservists, National Guard members, and new recruits to the U.S. Armed Services who have not yet been issued a DoD Identity (ID) Number, may authenticate with a DoD-approved non-DS Logon UN/PW to Sensitivity Level 1 information. Once these users are issued DoD ID Numbers, their UN/PW must be revoked, and they must be issued a DS-Logon and CAC.

E. Students in Schoolhouse Environments. Students in schoolhouse environments may authenticate with a DoD-approved non-DS Logon UN/PW to “Recruit, Train, and Equip” content that is low-risk and non-sensitive.

F. Medical Devices. Users may authenticate to certain medical devices with a DoD-approved non-DS Logon UN/PW.

II. **Secret Classified DoD IS Residing on Secret Classified DoD Networks**. For these use-cases, privileged users must authenticate with SIPR Admin-I tokens or DoD-approved MFAs.

A. DoD Non-DEERS Users. These users must follow the direction in the DoD CIO Memorandum, "SIPRNet PKI Tokens for Contractor SIPRNet Enclaves." Since the memorandum was signed, 90meter, Inc. has developed the capability for non-Microsoft Active Directory (AD) environments to support PKI network crypto-logon to the SIPRNet. DoD sponsors of non-AD connections must now configure the connections to require user network crypto-logon with DoD NSS SIPR PKI tokens.

B. FVEYs on the SIPRNet. FVEY users accessing the SIPRNet via UN/PW are authorized uninterrupted access via the SIPRNet REL DMZ account management process until the deadlines for their respective nations in the DoD CIO Memorandum, "Requirements for the FVEY Nations to Establish PKI Interoperability with DoD Classified Networks." This access is granted as an interim solution while FVEY partners complete development, testing, and validation for PKI-based authentication to the SIPR REL DMZ proxy.

C. SIPRNet Other. U.S. CYBERCOM FRAGORD 2 to TASKORD J3-12-0863 permits UN/PW authentication for several SIPRNet use-cases, and grants DoD CIO authority to update guidance on these use-cases (and require stronger authentication) as solutions become available. When the FRAGORD and this memorandum conflict, this memorandum shall take precedence. For example, regardless of what the FRAGORD states, DoD Components must require strong authentication for:

1. DoD systems that can support DoD-approved MFA or IFS, even if they cannot support PKI.

2. DoD unclassified users ineligible for or unable to obtain PKI, but eligible for and able to obtain DoD-approved MFA or IFS.

III. **Unclassified and Secret Classified DoD IS on Unclassified and Secret Classified DoD Networks**. Unless stated otherwise, these use-cases apply to both privileged and authorized users.

A. Stand-alone Networks and Systems. A stand-alone network is not connected to any other network, and does not transmit, receive, route, or exchange information outside of the network's authorization boundary. DoDI 8500.01 defines stand-alone systems. DoD AOs should require the strongest feasible authentication methods for these networks and systems, but may allow DoD-approved non-DS-Logon UN/PW.

B. Closed Restricted Network (CRN). A CRN is a closed Type IV system enclave not logically connected to any other global system or network, such as the Internet, NIPRNet, or SIPRNet, but that cryptographically tunnels over one or more of these networks for transport purposes. CRN traffic must be encrypted end-to-end over the transport network using DoD-approved cryptography. DoD AOs should require the strongest feasible authentication methods for these networks, but may allow DoD-approved non-DS-Logon UN/PW.

C. Platform Information Technology (PIT). DoD Components shall consult with DoDI 8500.01 and DoDI 8510.01 regarding authentication and other cybersecurity requirements for PIT.

D. Lab and Testing Environments. DoD Component may permit DoD-approved non-DS-Logon UN/PWs to be used in lab and testing environments that wholly or partially are isolated from the DoD Information Network (DoDIN). Many of the systems in these environments are either immature, still in development, or perform testing for the purposes of system validation, and PKI, MFA, and IFS are infeasible. At a minimum, these systems must operate in an OOB environment with no email or web access capabilities. Once a system is ready to be put on the DoDIN, it must be brought into compliance with strong authentication and other cybersecurity requirements as part of the Authorization to Operate (ATO) process.

E. Emergency, Backup, and Local Logon Accounts. DoD Components may permit DoD-approved non-DS-Logon UN/PWs to be used for authentication to these types of privileged accounts, when required to do so by applicable Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs) or Security Requirements Guides (SRGs).

1. Emergency Accounts are established in response to crisis situations. The accounts must be automatically deactivated after a preset amount of time.

2. Backup accounts are able to read and write to any file in a system. Due to these privileges, these accounts must be closely tracked.

3. Local Logon Accounts are used when network or normal logon/access is unavailable. They must not be used at any other time.

F. Tactical, Deployed, or Low Bandwidth Environments. There are certain deployed or tactical environments or situations where either the system or the network infrastructure cannot support DoD-approved PKI, MFA, or IFS, or the user cannot obtain DoD-approved PKI, MFA, or IFS. The base commander or on-site commanding officer may authorize the issuance of DoD-approved non-DS-Logon UN/PWs to users operating in these environments. Base commanders or on-site commanding officers must:

1. Determine feasibility of supporting PKI, MFA, or IFS based on operational risk, warfighter safety, and available IT infrastructure.

2. Direct and enforce limits on which networks, systems, and information the tactical, deployed, or low bandwidth users can access with UN/PW.

3. Ensure the SO or AO of relying parties are briefed on the situation and user-requirements for access to their systems.

4. Revoke user's UN/PW after the user is redeployed from the tactical, deployed, or low bandwidth environment.