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



MEMORANDUM FOR CHIEF MANAGEMENT OFFICER OF THE DEPARTMENT OF DEFENSE
SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
CHIEF OF THE NATIONAL GUARD BUREAU
GENERAL COUNSEL OF THE DEPARTMENT OF DEFNSE
DIRECTOR OF COST ASSESSMENT AND PROGRAM EVALUATION
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
DIRECTOR OF OPERATIONAL TEST AND EVALUATION
CHIEF INFORMATION OFFICER OF THE DEPARTMENT OF DEFENSE
ASSISTANT SECRETARIES OF DEFENSE FOR LEGISLATIVE AFFAIRS
ASSISTANT TO THE SECRETARY OF DEFENSE FOR PUBLIC AFFAIRS
DIRECTOR OF NET ASSESSMENT
DIRECTORS OF DEFENSE AGENCIES
DIRECTORS OF DOD FIELD ACTIVITIES

**SUBJECT**: Authorizations to Operate Extensions and Cybersecurity Function Prioritization Guidance

The COVID-19 pandemic is creating and disrupting significant portions of the Department's daily operations. Restrictions on travel and forced telework have made Assessment and Authorization efforts extremely difficult. Questions have arisen regarding cybersecurity requirements for Department of Defense (DOD) systems and the handling of expiring Authorizations to Operate (ATO) in the face of mandated telework and restrictions on traveling. This memo provides direction to Services and Components in dealing with expiring ATOs and determining mission essential functions and personnel required should the Department move to a Health Protection Condition (HPCON) Delta status.

**Authorization and Assessment Guidance**

Any new Operational Risk Assessments (ORA) and ATO for expanded telework capabilities must be authorized and approved by USCYBERCOM and DoD Chief Information Officer (CIO).

Systems and components have requested guidance on expiring authorizations during the current condition. Authorizing Officials (AOs) should identify systems with authorizations that are expiring in the next 30, 60 and 90 days. Blanket waivers should be avoided. These waivers do not reflect the Department's policy of actively managing operational risk. Once systems are identified, AOs should look at the cybersecurity posture of these systems and triage these systems based on operational priorities, vulnerabilities and threat exploitation. Component CIOs should have visibility in to the number of systems being extended and the associated impacts. AOs will report bi-weekly to their component Senior Information Security Officer (SISO) on systems that must be delayed within their 30/60/90 day windows to ensure visibility of the risk being accepted. Additional guidance and other factors that must be considered are contained in Appendix A.

**General Cybersecurity Requirements, Priorities and Best Practices**

Responding to the current exigent circumstances will require senior leaders, commanders/directors at all echelons and their cybersecurity experts to manage risks within operational and workforce realities. Ensuring the safety and health of our workforce is critical. AOs must work with their commander/directors to prioritize efforts against workforce and operational constraints. To achieve this, open and ongoing collaboration between AOs, systems professionals and component cyber forces is essential to ensure that cyber risks are balanced appropriately against operational and workforce constraints. AOs should leverage their normal channels to make threat –informed decisions. Component cyber officials may fill the void when normal channels are reduced due to the national emergency.

**System Activity Prioritization**

Decision makers, Commander/Directors, AOs, systems and organizations must work together to ensure that system operations are prioritized to minimize disruptions to the Department. As such, essential personnel should include those individuals necessary to maintain system operations and security. Additionally, secure, remote administration capabilities should be leveraged to the greatest extent possible if personnel have been trained on using this configuration and infrastructure is compliant with current directives. Additional guidance is contained in Appendix B.

**Cross Domain Solutions**

Cross Domain Solutions (CDS) are critical technologies that are mission essential and any interruption or degradation of their capability poses significant risk to the Enterprise. Due to the operation, nature of their work, cybersecurity measures need to be maintained at highest levels to protect valued data. As such, the operation maintenance and authorization of these systems and technologies should be considered mission essential. Patching CDS should be a high priority. Patching CDS should not open the environment or the system to outside automated connections. Files being brought into this environment should be thoroughly scanned.

**Conclusion**

Successfully navigating the current emergency situation while maintaining the minimal acceptable operational risk posture of the Department will require new levels of coordination among supporting processes, teams and disciplines. Communication, documentation, and tracking of risks, threats and mitigations across all disciplines will be essential to our success. This is critical as when this situation normalizes, we will be required to prioritize cleanup activities for the exceptions that were accepted temporarily. Senior Leaders, Commander/Directors, Component cyber forces and cybersecurity experts should coordinate together to determine priorities and understand the reasoning for those priorities.
Further guidance will be posted to the Risk Management Framework Knowledge Service https://rmfks.osd.mil. The point of contact for this matter is Mr. McKay Tolboe at mckay.r.tolboe.civ@mail.mil, (571) 372-4640.

WILMER.JOHN.W.III.1267975430

Digitally signed by WILMER.JOHN.W.III.1267975430
Date: 2020.04.03 12:54:07 -04'00'

John W. Wilmer
DOD Senior Information Security Officer

Attachments:
Appendix A – Authorization and Assessment Guidance
Appendix B – System Activity Prioritization

# Appendix A.

**Authorization and Assessment Guidance**

AOs should consider the following factors when extending the authorization.

- System Continuous Monitoring (CONMON) – AOs should take into account the automated CONMON capabilities of their systems. CONMON should be leveraged to the greatest extent possible to provide real time situational awareness of the system. Automated pushes of HBSS and ACAS scans can be set up via HBSS ePO or ACAS Security Center system affiliation tag. At a minimum, manual uploads of scans can be accomplished to DoD Centralized repositories (e.g., eMASS, MCAST, etc.) to provide situational awareness. Increased usage of these centralized repositories can enable collaboration and allow components to better manage risks within component environments.
- Physical Assessment security controls – Certain controls can only effectively be assessed by physical inspection. The physical security family of controls is a good example. Where appropriate, AOs can identify security controls that have to be assessed physically and issue authorization with the condition that those controls be assessed at the soonest possible time.
- Patching and POA&M compliance – The risk assessment of a system should include the ability of the system owner to proactively identify issues and resolve those issues. Systems that have demonstrated a trend of their inability to patch, maintain secure configurations, or meet POA&M timelines pose a risk to the Department and unless mission critical should not have their ATO extended.
- Type and Interconnections of the system – certain types of systems and the extent of their interconnections pose greater risk to the Department than other types of systems. Very broadly, these system can be classified as Unclassified External Facing, Unclassified Internal Facing, Classified and stand alone.
    - **Unclassified External Facing** – These systems include connections to the Internet and pose the highest risk of the four categories. Secure, remote administration should be leveraged to the greatest extent possible if personnel have been trained on using this capability and infrastructure is compliant with current directives. These systems should maintain updated patching to the greatest extent possible. These systems should already be residing in a DMZ and the posture of the DMZ should be considered.
    - **Unclassified Internal Facing** – Unclassified internal facing systems that do not have direct external connections to the internet. However, these systems exist on networks with systems that do have connections to the internet. This scenario may allow adversaries to laterally move, or pivot into these systems. These systems frequently have secure remote administration capability, which should be leveraged to the greatest extent possible if personnel have been trained on using this capability and infrastructure is compliant with current directives. It is still critical for these systems to continue to patch. System cybersecurity posture,

defense in depth and threat information (classified and unclassified) should all be evaluated to identify priority patching efforts.

- **Classified Systems and Networks** – Classified systems and networks generally are insulated from direct internet connections. Patching efforts should focus on cross domain solutions and remote exploit vulnerabilities. However, these systems have minimal/no remote administration capabilities. Effective integration with Cyber Security Service Provider (CSSP) and cyber mission forces is critical for determining the correct prioritization for patching efforts.
- **Standalone Systems and Networks –** Standalone systems and networks have no connections outside of their authorization boundary. As such, there are significant mitigations in place protecting those assets. Priority should be given to maintaining their disconnected status.
- **Cross Domain Solutions -** Cross domain solutions patching should be a high priority. Conducting patching should not open the environment, or the system to outside automated connections. Files being brought into this environment should be thoroughly scanned.

***NOTE:*** *For systems under ATOs that are granted waivers within in the unclassified external facing or unclassified internal facing categories AND determined to have VERY HIGH cybersecurity impacts (examples: open non-standard ports/protocols in the boundary, weak encryption, non-compliance trends, etc.) JFHQ-DODIN will require a truncated ORA, to track continued risk posture impacts until they can be resolved.*

## Appendix B.

**System Activity Prioritization**

The following activities should be considered mission essential functions and be considered in designating mission essential staff:

- **Operations:** Cybersecurity is intended to ensure that the confidentiality (C), Integrity (I) and Availability (A) of a system and its data. As such, system personnel who are essential to maintaining the operation of systems are essential. System personnel include help desk technicians who assist users with resolving system issues and problems.
- **Account Management:** Account management is a critical operational and cybersecurity function. Components, networks and systems need to evaluate the impact of teleworking on their user base to determine whether existing rules for inactivity are feasible. If a large percentage of the user base cannot access a system due to telework, AOs may make a risk decision to extend the inactivity time before disabling an account; defined in the DOD Security Requirements Guides as being 35 days, along with the timeline for deleting an account which is specified in DOD SRGs as 60 days. This decision should be made in consultation with component cyber forces.
- **Assessment and Authorization**: Systems should maintain their cybersecurity posture at all times to ensure warfighter/business operations can continue with minimum risk. Authorizing Officials should leverage the systems continuous monitoring plans and its results to continually manage risks associated with system authorizations. AOs should work with their commander/director to better understand the overall risk of the system. Internet facing systems inherently carry more operational risk than internal facing, or standalone systems. When making decisions on ATOs and their extensions, components should take a risk managed approach, rather than issue blanket waivers. Considerations include:

    - **Incident Management** – Systems must be able to respond to any incidents that may occur that affect the C, I and A of a system or its data.
    - **Secure Configuration Management** – Developing and maintaining a secure system configuration is an important step in minimizing operational risk. Maintaining these secure baselines is essentials towards maintaining adequate system risk postures. Failure to maintain a secure configuration can introduce significant vulnerability and risk into a system.
    - **System Monitoring** – System continuous monitoring capability is essential in providing situational awareness for cyber defense and risk management. A loss, or degradation in this capability reduces the Department's understanding of real-time risks associated with systems, or identifying cyber intrusions.
    - **Patch Management** – Systems must continue to be patched where feasible. Prioritization for patching should be based on two factors: 1) how important is the system to getting the Component mission accomplished and 2) how likely will threats exploit the vulnerability. Vulnerabilities that have remote access are high targets for threat exploitation should be given priority for patching. JFHQ DoDIN's patching alerts, which include the CVSS score and a threat informed prioritization

methodology in their daily Cyber Tasking Order provide significant details for patching priorities. Additional details through commercial, unclassified and classified intelligence reporting should also be considered as well as risk in consideration of an ATO extension.