COVID-19 Telework Talking Points

"In this unprecedented time for our nation, DoD networks remain fully capable of supporting the mission critical duties necessary to execute our missions. We are fully committed to maximizing the use of a telework-ready IT environment to ensure the health and welfare of our personnel given the ongoing COVID-19 pandemic. As teleworking increases, we are working diligently to advance the capability and capacity of our network posture to support the rise in demand. Securing and defending DoD networks is a 24/7 mission and cybersecurity will always remain a top priority."

The Honorable Dana Deasy, DoD Chief Information Officer

Key Messages:

- The health of DoD military, civilians and contractor personnel is the Secretary of Defense's number one priority as we fight the threat from COVID-19.
- On March 12, OMB signed a memorandum providing civilian personnel policy guidance in response to the coronavirus.
- All federal executive branch departments and agencies, including DoD, are offering maximum telework flexibilities to all current telework eligible employees consistent with the operational needs of the departments and agencies. The White House has also encouraged agencies to offer telework flexibilities to eligible workers identified by the CDC as being at higher risk for serious complications.
- DoD is maximizing the use of telework for those employees who are telework ready in order to decrease the spread the COVID-19 virus.
- DoD networks are telework ready and capable to fully support the mission critical duties performed by the department.
- DoD has expanded the network capacity due to the unprecedented demand for telework capabilities.
- Defending DoD networks is a 24/7/365 mission which will never cease. Cyber security will remain a top priority.
- DoD personnel are trained annually about cybersecurity threats such as phishing and should continue to practice good cyber hygiene while working in the office, or teleworking.

Telework Ready Workforce

- The White House provided updated guidance for the National Capital Region on telework flexibilities in response to the Coronavirus (OMB Memo 20-15). All federal executive branch departments and agencies are asked to offer maximum telework flexibilities to all current telework eligible employees consistent with the operational needs of the departments and agencies. The White House additionally encouraged telework flexibilities to eligible workers identified by the CDC as being at higher risk for serious complications (OMB Memo 20-13).

- The Secretary of Defense has given commanders the authorities they need to make necessary decisions to protect their forces. Commanders are empowered to take necessary precautions because the COVID-19 is unique to every situation and every location.

- Telecommuting is one of the options commanders have to protect service members while still safeguarding and maintaining our ability to defend the nation and its interests. There are multiple options to telecommute, including using government cell phones, laptops and remote desktop support.

- We are maximizing the use of remote work for those personnel who are telework ready and authorized to work remotely to decrease the spread of infection of COVID-19. Additionally, if need be, an agency can mandate that an employee telework even if the employee is not on a telework agreement, as part of its continuity of operations plan (COOP).

- Telework arrangements for the Pentagon will allow personnel to perform work, during any part of regular, paid hours, at an approved alternate worksite (e.g., home, alternate site) to focus on mission readiness.

- The DoD networks are ready to support the mission critical duties that need to be performed by the Department in a telework-focused environment.

- Due to the dynamic nature of the COVID-19 response, we continue to review and assess our capacity and capability to accommodate teleworking at scale.

Mitigating Cyber Threats

- Personnel must practice strong cyber hygiene and operational security awareness while online to ensure the department networks stay secure.

- We have disseminated clear guidance that the same discipline, awareness, and security measures required for on-site work must be observed by our personnel when working remotely.

- DoD networks will not be able to stream music or video applications unless it's for mission-critical activities.

- In addition to our routine cybersecurity activities, we have stood up a Technical Capability Task Force comprised of DoD CIO, USCYBERCOM, JFHQ-DODIN, NSA, DISA, Joint Staff, and the Military Services continue to focus on the network readiness of the Department.

- This Task Force meets daily and is closely monitoring the IT environment across the Department and executing cybersecurity measures to ensure the confidentiality, integrity and availability of the network for our warfighters.

FAQ-COVID-19 Telework

Q: Is DoD taking additional measures to expand network access to those working remotely?

A: DoD networks are ready to support the mission critical duties performed by the department. Due to the current increased remote work demands, the Department will eliminate the capability to stream video and music on DoD networks, except for mission critical activities.

Q: Are the DoD networks experiencing problems due to the amount of telework? What about the rumors personnel cannot connect well at home? Is the department looking at alternate commercial-based telework solutions?

A: We are in an unprecedented time for our nation. The DoD networks remain fully capable of supporting the mission critical duties necessary to execute our missions. We continue to diligently advance our capabilities and capacity of our network posture to support the demand.

> ***If Pressed:*** *The Department is constantly evaluating the capabilities and capacity of our remote work solutions against the unprecedented demands we are experiencing. We are engaged with our partners in industry and evaluating solutions through a dedicated team to ensure the Department can execute our mission without interruption. DoD CIO is leading this engagement.*

Q: Although the Pentagon is open, are most employee's teleworking?

A: The Pentagon and other DoD facilities in the National Capital Region will remain open and operational, however, the DoD is maximizing the use of remote work capabilities for those personnel who are telework authorized and ready in order to decrease the spread of infection. DoD is using remote work as a means of social distancing while creating separation for those who must be at the Pentagon or other DoD facilities. It's all about accomplishing the mission while protecting the force.

Q: How many Civilians or uniformed officers are teleworking? Are they able to remotely access DOD networks via personal devices or only from government-issues devices?

A: The Department will not provide a specific number for teleworking personnel. The Secretary of Defense has given commanders the authorities they need to make necessary decisions to protect their forces. Commanders are empowered to take necessary precautions because the virus is unique to every situation and every location. Teleworking is one of the options commanders have to protect service members while still maintaining our ability to defend the nation and its interests. There are multiple options to telework, including using government cell phones, laptops and remote log-in devices.

Q: Will DoD missions be impacted by telework?

A: DoD employees with telework agreements are capable of successfully executing their missions remotely. DoD networks will remain secure and able to support mass telework during COVID-19. Employees who need to be in the office will practice social distancing.

Q: Will DoD have the resources to support mass telework for several weeks?

A: The DoD will be able to support mass remote work capabilities for as long as deemed necessary for the safety of DoD personnel and their families due to COVID-19.

Q: What is the Department doing differently to handle the telework issues that arise during the COVID-19 pandemic?

A: The DoD CIO stood up a dedicated Technical Capabilities Task Force which includes a number of key players: DoD CIO, USCYBERCOM, JFHQ-DODIN, NSA, DISA, Joint Staff, and the Military Services This task force meets daily to assess and identify solutions to issues that have arisen due to the need for increased telework capabilities and capacity.

Q: What steps are being taken to ensure network security? Are VPNs being used or other remote access measures? Will additional steps be taken if more employees are restricted from entering the Pentagon?

A: Cyber and network security are a key priority for the department. Service members are fully trained on information security and best practices, including the annual training requirements. Defending DoD networks is a 24/7/365 mission, which will

not cease, even as the Department of Defense's top priority remains the protection and welfare of our people.

Q: Where can people find more information about protecting their networks?

A: During the pandemic we must remember to practice good handwashing hygiene, but also remember our cyber hygiene habits. DoD personnel regularly take training about cybersecurity and can read more about online safety here: **https://cyber.mil** or **https://public.cyber.mil**