EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

DEPUTY DIRECTOR
FOR MANAGEMENT

March 22, 2020

M-20-19

MEMORANDUM FOR HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Margaret M. Weichert
Deputy Director for Management

MARGARET WEICHERT
Digitally signed by MARGARET WEICHERT
Date: 2020.03.22 10:37:58 -04'00'
X
Margaret Weichert
Deputy Director for Management

SUBJECT: Harnessing Technology to Support Mission Continuity

As our response to the national emergency for the coronavirus disease 2019 ("COVID-19") continues to evolve, the Administration directs that agencies utilize technology to the greatest extent practicable to support mission continuity.

Over the past several years, agencies have been making significant investments in technology infrastructure, scalable technology platforms and digital delivery of mission support and mission delivery functions. In some situations, although technical capabilities are available, agency business processes have not evolved to fully utilize these expanded capabilities. By aggressively embracing technology to support business processes, the Federal Government is better positioned to maintain the safety and well-being of the Federal workforce and the American public while supporting the continued delivery of vital mission services.

In response to the national emergency for COVID-19, agencies are directed to use the breadth of available technology capabilities to fulfill service gaps and deliver mission outcomes. The attached set of “frequently asked questions” are intended to provide additional guidance and further assist the IT workforce as it addresses impacts due to COVID-19. Additional technology-related questions should be directed to the Office of the Federal CIO at OFCIO@omb.eop.gov. OMB will continue to provide updates and additional information as needed to support the resiliency of agency missions.

Attachment

Attachment

Harnessing Technology to Support Mission Continuity
Frequently Asked Questions

1. **What flexibilities do agencies have to adjust operations to support mission delivery?**

   OMB issued M-20-16, Federal Agency Operational Alignment to Slow the Spread of Coronavirus https://www.whitehouse.gov/wp-content/uploads/2020/03/M-20-16.pdf, which provides an overarching directive with broad latitude to provide maximum flexibility to agency leaders.

2. **How should agencies confirm that both internal users, and the public are positioned to leverage an agency's digital service offerings?**

   Agencies are encouraged to update their .gov websites to the greatest extent practicable to provide agency service delivery information to Federal Government consumers and to direct Federal Government consumers to the appropriate digital and telephonic resources to obtain needed services. We also encourage agencies to assess the usability of its digital resources, and to improve user centered design and customer service aspects of its websites, web applications, and other citizen-facing interfaces.

   Additional Resources:
   - OMB M-17-06, Policies for Federal Agency Public Websites and Digital Services
   - Guidance on building better digital services in Government, https://digital.gov/resources/

3. **What can agencies do to better facilitate personnel productivity in a remote environment?**

   Agencies are encouraged to leverage agency approved collaboration tools and capabilities to the greatest extent practicable. This action may include increasing the number of licenses available, leveraging services and technologies across the enterprise, and directing specific activities to be conducted via collaboration forums. Additionally, it is recommended that agencies make use of collaboration tools and capabilities offered by other Federal agencies to meet capability gaps. Such use cannot override legal terms of service.

   Additional Resources:
   - Federal-Compatible Terms of Service Agreements
   - List of free tools that have federally-compatible negotiated Terms of Service
   - General Services Administration's (GSA's) Consolidated Federal Supply Schedule offers pre-negotiated terms of services agreements

4. What should agencies do when remote workers need to print and sign forms?

Agencies should continue to follow existing policies on the usage of personal printers and external media. Agencies are encouraged to leverage digital methods to meet mission needs, to include leveraging digital forms and electronic signatures to the fullest extent practicable. When evaluating the Paperwork Reduction Act considerations associated with changes to a form or its content, contact OMB OFCIO or your OMB Office of Information and Regulatory Affairs desk officer to remove impediments that may slow adoption of any new or revised information collection method. It is recommended that agencies identify any impediments to using digital signatures, and remove those impediments, consistent with applicable law. OMB should be notified about any impediments that cannot be adequately addressed. In addition, agencies should consider leveraging digital signature capabilities offered by other Federal agencies to meet any technological capability gaps.

Additional Resources:

- OMB M-19-17, Enabling Mission Delivery through Improved Identity, Credential, and Access Management
- OMB M-00-15, Guidance on Implementation of the Electronic Signatures in Global and National Commerce Act (E-SIGN)
- M-00-10, OMB Procedures and Guidance on Implementing the Government Paperwork Elimination Act
- The Federal Chief Information Officers Council guidance, "Use of Electronic Signatures in Federal Organization Transactions"

5. Are agency cybersecurity and privacy requirements still applicable/what are some areas of focus?

Security protocols, requirements regarding the appropriate use of federal resources, and legal requirements are always applicable. However, agencies are encouraged to make risk-based decisions as appropriate to meet mission needs as outlined in M-20-16, Federal Agency Operational Alignment to Slow the Spread of Coronavirus https://www.whitehouse.gov/wp-content/uploads/2020/03/M-20-16.pdf. Areas of increased focus concerning cybersecurity and privacy include:

- Updating Virtual Private Network components, network infrastructure devices, and devices being used to enable remote work environments with the latest software patches and security configurations;
- Providing guidance to employees about how to ensure proper information security and privacy controls are in place when working from alternate locations or home;
- Continuing to prohibit the unauthorized forwarding of Federal Government business materials or other information to personal devices;
- Continuing to prohibit the unauthorized usage of social media platforms or any unauthorized devices for Government business; and
- Confirming that the expanded usage of technology tools is in accordance with appropriate legal considerations and does not violate legal terms of service.

Additional Resources:

- M-13-10, Antideficiency Act Implications of Certain Online Terms of Service Agreements
- Alert (AA20-073A): Enterprise VPN Security
- GSA's Consolidated Federal Supply Schedule offers pre-negotiated terms of services agreements
- GSA's Highly Adaptive Cybersecurity Services (HACS) Special Item Number (SIN) provides rapid access to key support services from technically evaluated vendors

6. What should agencies consider when managing physical access to facilities for personnel who have not been required to or may have be unable to access the facility?

When managing physical access to facilities, agencies should consider the following:

- Preparing to accommodate personnel who are issued a new PIV credential or that receive a PIV certificate update during their absence from Federal facilities, and who might need to re-enroll their PIV in the Physical Access Control System (PACS) for access to the facility.
  - PACS that have local non-use policies may require mass re-enrollment and/or re-activation of PIV credential facility access permissions.
  - Agencies may need to increase the number of staff needed to support re-enrollment.
- Proactively scheduling appointments for users to complete re-enrollment activities.

7. Per the Office of Personnel Management's (OPMs) soon to be released guidance, agencies have the ability delay the completion of fingerprinting requirements based on an agency's risk determination and the need to onboard mission-critical personnel. Am I required to issue new personnel a PIV credential?

Agencies are able to make a risk determination and issue an alternate credential/authenticator for PIV eligible personnel due to the inability to collect biometrics (e.g., fingerprints), until biometric processing is feasible.

- Agencies should consider impacts to both physical and logical access when determining to issue a PIV eligible user an alternate credential/authenticator during this period of time.
- Issuance of an alternate credentia/authenticator should be tracked and a process should be established to prioritize the issuance of a PIV credential to the affected individual upon the restoration of normal business practices.

Additional Resources:

- OPM guidance, Final Credentialing Standards for Issuing Personal Identity Verification Cards under HSPD-12

8. **What should agencies do if they are unable (e.g., low on card stock, unable to complete PIV enrollment activities) to reissue a PIV credential to personnel?**

   Agencies are encouraged to work with OMB and GSA to help resolve any issues with PIV credential issuance. If agencies are unable to issue a PIV credential, they should be prepared to issue an alternate credential / authenticator for physical and logical access.

   - Agencies should consider impacts to both physical and logical access when making a risk determination on issuing a PIV eligible user an alternate credential / authenticator.
   - Issuance of an alternate credential / authenticator should be tracked and a process should be established to prioritize the issuance of a PIV credential to the affected individual upon the restoration of normal business practices.

   Additional Resources:
   - GSA's Identity, Credentials and Access Management Program Information

9. **What should agencies consider when managing access to IT systems for personnel who have not been required to or may have be unable to access the network or specific applications?**

   Agencies are encouraged to consider the following for managing access to IT systems following an extended absence from Federal facilities:

   - Depending on agency non-use policies and configurations, enterprise domain/network accounts and authenticators for users may expire or be disabled due to non-use.
     - Identifying whether enterprise domain / network account authenticator (where a PIV credential is not in use) requires re-issuance (e.g., token) or reset (e.g., password).
     - Identifying accounts disabled during an absence from federal facilities, and proactively completing an account recertification with account authorizers to enable reinstatement.
   - Identifying whether any Federal Government IT equipment with local user accounts will require enablement or authenticator re-issuance/reset.
     - Depending on agency non-use policies and configurations, access permissions for Government IT equipment may automatically be disabled after a period (e.g., 30 days).
     - Where possible, remind users to access their Government IT equipment before the agency defined expiration date to maintain access, during an absence from Federal facilities.
   - Preparing Service Help Desk surge staffing to accommodate increased volume for IT requests.
     - It may be necessary to prioritize ticket requests based on mission need.
     - Agencies should ensure if the user is not in-person for account actions that they verify the user's identity to remain vigilant against social engineering attacks.