The Digital Worker Identity Playbook

Guidance to Secure Your Agency's Digital Workforce

January 5, 2021
FINAL

Identity Assurance and Trusted Access Division

General Services Administration
Office of Government-wide Policy

Table of Contents

Executive Summary

The Digital Worker Identity Playbook is a practical guide to manage digital worker identities. This playbook helps federal agency ICAM programs as well as CIO and CISO offices determine the risk of and define a process for digital worker identity management. A digital worker is an automated, software-based tool, application, or agent that performs a business task or process similar to a human user and uses Artificial Intelligence (AI) or other autonomous decision-making capabilities. OMB memo 19-17 requires agencies to ensure the digital identity of automated technologies are "distinguishable, auditable, and consistently managed." However, agencies face implementation challenges when establishing identities for digital workers. Most often, they attempt to use human worker processes, which may hinder digital worker creation or access. Common challenges include:

- Human worker identity attributes that do not apply to a digital worker. For example, some agencies create ad hoc digital worker identity attributes based on requirements for human users, some of which do not apply (e.g., work station location). Conversely, the scope of identity attributes required for human users may not include some attributes that are needed for digital workers (e.g., custodian names).
- Lack of ability to provision individual user accounts to a digital worker. Some agencies allow digital workers to run on service, system, or group accounts. This is because implementation teams are either unable or not authorized to have individual user accounts assigned to a digital worker. However, digital workers are less distinguishable from other non-person entity types when they use service, system, or group accounts rather than user accounts.

Agencies should tailor this playbook to fit their mission, business, technology, and security needs and integrate into enterprise identity management policies.

Federal agencies use digital workers to automate processes, increase efficiencies, and discover insights from large volumes of data. Digital workers may interact with or use sensitive information to perform unattended, high-risk tasks, which may critically impact an agency's mission. Agencies usually leverage existing, human-based processes to create a digital worker identity, but this may hinder a digital worker's access or success. This playbook addresses the challenges in determining digital worker risk and outlines a process to establish a digital worker identity.

This playbook is iterative, and agencies are encouraged to collaborate, share best practices, and lessons learned. Federal employees may consider joining a relevant committee or community of practice to learn and engage in digital worker identity management.

- [Identity, Credential, and Access Management subcommittee (ICAMSC)](#)
- [Robotic Process Automation Community of Practice](#)

- [Artificial Intelligence Community of Practice](#)

Key Terms

These are key terms used throughout this document.

- **Digital Worker** - An automated, software-based tool, application, or agent that performs a business task or process similar to a human user and uses AI or other autonomous decision-making capabilities.[1]

The list below includes the most common types of digital workers.

- **Artificial Intelligence (AI)** - A computer system's ability to make autonomous decisions or perform tasks, traditionally requiring human intelligence.
- **Chatbot** - A software tool that interacts with a human user to provide a service, such as retrieving data, answering a question, or directing the user to a resource.
- **Machine Learning (ML)** - The process of teaching computers to learn from data and perform tasks with minimal direct instruction or programming on how to achieve the desired outcome.

Disclaimer

This playbook was developed by the General Services Administration Office of Government-wide Policy with input from federal IT practitioners. This document shouldn't be interpreted as official policy or mandated action, and doesn't provide authoritative definitions for IT terms. Instead, this playbook supplements existing federal IT policies and builds upon the Office of Management and Budget (OMB) Memorandum 19-17 (M-19-17), *Enabling Mission Delivery through Improved Identity, Credential, and Access Management* and existing federal identity guidance and playbooks. Subject areas with intersecting scope, such as the ethical use and development of digital workers, are considered only to the extent that they relate to digital identity management and credentialing for digital workers. Specific security control implementations are out of scope of this playbook, as are any elements of data protection requirements and the suitability process for a digital worker sponsor and custodian.

---

[1] Digital worker is not synonymous with non-person entity (NPE), as NPE encompasses all entities with a digital identity including organizations, hardware devices, software applications, and information artifacts.

A Three-Step Process for Digital Worker Identity Management

The three-step process outlined below is a structured, iterative approach with discrete actions to create a digital worker identity management process. **CIO and CISO offices** are the intended audience for this guide. Use this guide to write, update, or enhance existing enterprise identity management policies. Agencies are encouraged to tailor these steps to meet organizational structures, unique requirements, and mission needs.
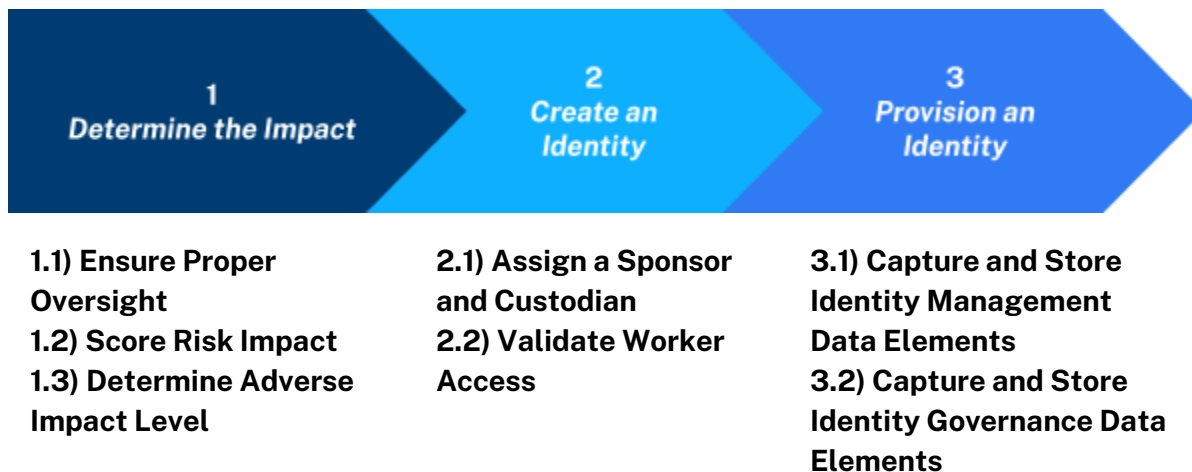

1 Determine the Impact	2 Create an Identity	3 Provision an Identity
1.1) Ensure Proper Oversight **1.2) Score Risk Impact** **1.3) Determine Adverse Impact Level**	**2.1) Assign a Sponsor and Custodian** **2.2) Validate Worker Access**	**3.1) Capture and Store Identity Management Data Elements** **3.2) Capture and Store Identity Governance Data Elements**

Figure 1. A Three-Step Process for Digital Worker Identity Management

Step 1: Determine the impact to decide whether to establish a digital worker identity. Much like the human worker, a digital worker should undergo a similar vetting process before being granted network or application access. Not all digital workers may require a unique identity. Work with the agency's ICAM governance structure[2] to:

- Create or expand the agency ICAM governance structure and policies for digital worker identity management oversight;
- Score risk using the Digital Worker Impact Assessment; and
- Identify a digital worker adverse impact level.[3]

The Digital Worker Impact Evaluation Matrix is a scoring tool. It uses six factors to score the risk of a digital worker's scope and access. Agencies can use the risk score to determine an overall adverse impact level.

---

[2] OMB Memorandum 19-17 instructs federal agencies to "designate an integrated agency-wide ICAM office, team, or other governance structure in support of its Enterprise Risk Management capability to effectively govern and enforce ICAM efforts.

[3] The adverse impact levels are grounded in NIST Special Publication 800-30, Guide for Conducting Risk Assessments, but do not align with it. Agencies can adjust the impact levels to match agency risk tolerance.

Key Point	Agencies may decide that Digital Workers with low adverse impact levels do not require a digital identity. If an agency's policy demands that all digital workers require a digital identity, they should follow the Moderate level process.

Step 2: Create an identity that complies with the agency ICAM policies. A digital worker is assigned a sponsor and custodian that maintains the digital worker processes. The sponsorship process creates and assigns digital worker oversight roles and responsibilities for a sponsor and a custodian. After appointing a sponsor and custodian, follow security best practices when validating a digital worker level of access. Best practices include employing least privilege, separation of duties, and regular access recertification, similar to human workers.

Step 3: Provision an identity in the agency enterprise identity management systems. After assigning a sponsor, custodian, and validating access, capture the appropriate data elements in the digital worker identity record. These data elements enable the agency to appropriately catalog and monitor digital workers through the identity lifecycle.

This playbook should aid agencies in integrating digital worker identity management processes into existing enterprise identity management policies.

Step 1: Determine the Impact

Ensure digital worker identity management has proper governance, score the function of the digital worker across six categories, and then use the risk score to arrive at an adverse impact level. For this step, we use the Digital Worker Impact Evaluation Matrix.

1.1 Ensure Proper Oversight

The ICAM governance structure ensures enterprise identity management policies are updated to include digital worker management and use. For ICAM oversight and program management examples, see the FICAM Program Management Guide.

Update the agency enterprise identity management policies to include digital worker identity management.

Governance Collaboration Example	Before creating and provisioning a digital worker, the agency ICAM governance structure can collaborate with Information System Security Officers on digital worker identity management. Collaboration may include: - Verifying digital worker security and non-functional requirements - Security and privacy assessments - Executable, vulnerability and other scans - Digital worker logic and decision-making design documents

1.2 Score Risk Impact

A risk score is calculated across six factors based on worker autonomy, content handled, type of access, and privileges required.

Each factor has an associated score, and the sum of these six-factor scores is the overall impact score. If multiple criteria within a factor apply to a digital worker, agencies should select the criterion with the highest score.

Table 1. Digital Worker Impact Evaluation Matrix[4]

Digital Worker Impact Evaluation Matrix Score each factor based on the most applicable scenario	
Factor 1 - Is the digital worker attended or unattended?	**Score**
● Attended	**0**
● Unattended	**10**
Factor 2 - What is the highest level of data access by the digital worker?	
● Data available to the public (either without a user account or with unvetted user account)	**0**
● Agency operational data, controlled unclassified information (CUI), or data on individuals in low volumes. Doesn't contain personally identifiable information (PII) or personal health information (PHI)	**5**
● PII and/or PHI	**55**
● Agency critical operational data or data that could impact life, health, or safety of individuals/systems relied upon for health and safety; or very high volumes of agency operational data	**90**
Factor 3 - Does the digital worker have access to internal and/or external networks?	
● No internal intranet or external internet connection	**0**
● Either internal intranet access only OR external internet access (not both)	**5**
● Internal and external network access (i.e., internet and intranet)	**10**
Factor 4 - What is the impact of the output generated by the digital worker?	
● Output impacts general internal business operations, but not for critical processes or decisions	**5**
● Output impacts outside organizations in general business operations or public reporting (e.g., public facing websites or chatbots), but not for critical processes or decisions	**25**

---

[4] For more information on the methodology used to develop the Digital Worker Evaluation Matrix, see Appendix A.

• Output impacts mission critical organization operations of the agency or other organizations, health or safety of individuals, national economic stability, national security, critical infrastructure, or similarly consequential operations	**90**
Factor 5 - What type of system account privileges does the digital worker require?	
• No system accounts used	**0**
• Standard system account(s) (roles limited by the business function)	**10**
• System admin account (privileged access)	**35**
• Multiple system admin accounts (multiple privileged access roles)	**40**
Factor 6 - Does the digital worker act on its own insights?	
• Digital worker develops insights, but doesn't take action on its insights	**0**
• Digital worker develops insights and acts on the insights after human review	**5**
• Digital worker develops insights and acts on the insights without human review or approval before the action is taken	**10**

1.3 Determine Adverse Impact Level

The adverse impact level is the potential magnitude of harm a digital worker can cause the organization, assets, individuals, other organizations, and the United States' economic and national security interests. Specific impacts include:

- unauthorized disclosure;
- change or destruction of information;
- harm or endangerment of human life;
- loss of access to information systems; or
- damage to high-value assets.

The four adverse impact levels represent a different scale of harm a digital worker may cause.
- Low;
- Moderate;
- High; and
- Critical.

Key Point	The Potential Adverse Impact Levels are grounded in NIST Special Publication 800-30 and are a recommendation. Agencies may adjust or tailor the levels to fit their individual risk levels or descriptions.

Table 2. Potential Adverse Impact Levels

Impact Score	Potential Adverse Impact	Description
0-35	Low	Effects of an error or accident are minimal, resulting in negligible, if any, impacts on organizational operations, finances, assets, individuals, other organizations, or the Nation.
36-55	Moderate	Effects of an error or accident are limited and may result in minor or temporary impact on organizational missions/business functions, organizational assets, or the Nation. This includes: increased difficulty in performing business operations in a timely manner, with sufficient confidence, or within planned resource constraints; minor damage to agency image, reputation, or trust; minor financial loss to the agency or other organizations; and/or noncompliance with applicable laws or regulations.
56-90	High	Effects of an error or accident are wide-ranging and could result in serious or long-term impact on organizational missions/business functions, organizational assets, or the Nation. This includes: significant financial losses for the agency; substantially reduced capacity to conduct mission critical business; loss of Personally Identifiable Information (PII), Business Identifiable Information, or Personal Health Information (PHI); and/or damage to agency image or reputation.
91+	Critical	Effects of an error or accident are extensive and will have severe or catastrophic impact on organizational missions/business functions, assets, or the Nation. This includes: major financial losses for the agency or other organizations; loss of government continuity of operations or ability to conduct mission critical business; life-threatening injury or loss of life; and/or harm to national security.
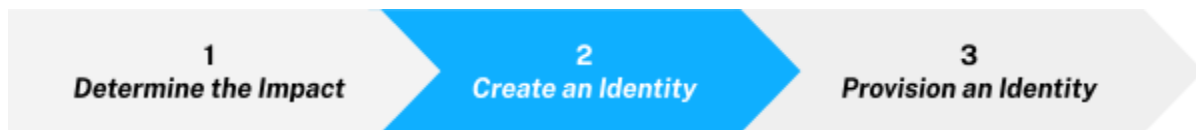
Step 2: Create an Identity

Once your agency has determined the digital worker's level of potential adverse impact, a digital worker identity is created, if needed. The identity process includes sponsorship and validation activities based on the adverse impact level from step 1.

2.1 Assign a Sponsor and Custodian

The sponsorship process allows agencies to assign specific roles and responsibilities for oversight of digital workers. The agency's ICAM governance structure ensures the sponsorship process actions are completed, however it is up to the individual agencies to define how a sponsor and custodian are assigned.

Table 6. Sponsor and Custodian Responsibilities

Role	Description	Responsibilities
Sponsor	- Responsible for digital worker compliance; and - A federal government employee.	- Assign roles and responsibilities to govern the digital worker such as a primary and backup custodian; - Field digital worker inquiries from agency or other government entity leaders; and - Oversee who has access to the digital worker.
Custodian	- Responsible for digital worker day-to-day operational management; and - A federal government employee or contractor.	- Holds a comparable level of access as the digital worker; - Completes initial and routine training in digital worker management and security; - Rotate digital worker password or authenticators; - Maintain digital worker access; - Oversee retraining or tuning of an underlying model; and - Track and monitor digital worker data input and output.

Industry Best Practice

Recertification or access reviews are assessed periodically if access privileges are still needed to complete a task and a minimum recommendation is required to verify and validate access. The recommended intervals in Table 7 for sponsor and custodian acknowledgment should be considered a minimum acceptable standard. Agencies may adjust the recertification frequency, but should meet or exceed the recommended intervals. When certifying human access to IT platforms, specific systems and applications may impact the frequency of necessary certifications. Agencies should assess the platforms that digital workers have access to and use this to help evaluate certification frequency.

Key Point	Agencies may decide that Digital Workers with low adverse impact levels do not require a digital identity. If an agency's policy demands that all digital workers require a digital identity, they should follow the Moderate level process.

Table 7. Sponsorship Process

Sponsorship (SP)					
ID[5]	Action	Low	Moderate	High	Critical
SP-1	**Document business need for the digital worker.**	N/A	✓	✓	✓
SP-2	**Assign an organizational sponsor for the digital worker.**	N/A	✓	✓	✓ Suggested CIO, CISO, or equivalent
SP-3	**Sponsor acknowledges responsibility for the digital worker on an initial and routine basis.**	N/A	✓ Recertify sponsor annually	✓ Recertify sponsor annually	✓ Recertify sponsor every six months
SP-4	**Sponsor assigns the custodian of the digital worker.**	N/A	✓	✓	✓
SP-5	**Notify the custodian of his or her responsibility by the sponsor.**	N/A	✓	✓	✓

---

[5] The ID number is specific to this playbook and does not map or correlate to requirements in other federal security publications.

SP-6	Confirm the custodian acknowledges responsibility for the digital worker on an initial and routine basis.	N/A	✓ Recertify custodian annually	✓ Recertify custodian annually	✓ Recertify custodian every six months

2.2 Validate Worker Access

Validation actions record the activities to ensure the digital worker continues to behave as expected throughout its lifecycle. The agency's ICAM governance structure is responsible for ensuring the validation process actions are completed and tracked, but the individual agencies must define a process that fits the agency's mission needs and requirements. Validation is based on the following factors as a starting point. Agencies may include other mission specific review factors as needed.

1. **Employ least privilege (VD-1).** Like a human worker, a digital worker should have the lowest access required to complete its task. The sponsor should review the use of an elevated account before initially granting it or upgrading an account already in use.
2. **Separation of duties (VD-2)** is a principle that prevents any single person or entity from completing all the functions in a critical or sensitive process. It is designed to "prevent fraud, theft, and errors." The sponsor should review that the digital worker role does not create a separation of duty conflict. If there is a conflict, document the exception.
3. **Code review (VD-3)**. Digital worker code may include worker logic and decision-making processes. Include design or other system documentation as part of code review for reasoning and decision-making intent.
4. **Ethics and bias review (VD-4 and VD-5)**. While government-wide standards for ethics and bias are in development, agencies should define their own ethics standards or collaborate with other agencies that align with the agency mission.
5. **Recertification acknowledgement (VD-6 and VD-7).** Recertification is the act of reviewing access on a periodic basis. It should occur on an annual or bi-annual schedule based on the adverse impact level.

Key Point	Existing validation activities can be leveraged and integrated into the digital worker validation process. Even though there are no activities for low impact, reassess a digital worker impact level every time there is a code change or update to ensure the impact level has not changed.

Use Table 8 for specific validation actions aligned with adverse impact level.

Table 8. Validation Process

Validation (VD)

ID	Action	Low	Moderate	High	Critical
VD-1	**Validate the digital worker role employs least privilege necessary to accomplish its task.**	N/A	✓	✓	✓
VD-2	**Validate the digital worker role doesn't create separation of duty conflicts for the digital worker or any human users.**	N/A	✓	✓	✓
VD-3	**Validate the digital worker has undergone a code review prior to release. Additional code reviews are required for any code changes at higher impact.**	N/A	✓ Following major changes to code	✓ Following any changes to code	✓ Following any changes to code
VD-4	**Validate the digital worker has undergone review of ethics according to applicable government and/or Agency standards.**	N/A	N/A	✓ Conduct initial review and annual periodic review	✓ Conduct initial review and periodic review every six months
VD-5	**Validate the digital worker has undergone review for bias according to applicable government standards.**	N/A	✓ Conduct initial bias review	✓ Conduct initial bias review and annual periodic review	✓ Conduct initial bias review and periodic review every six months

VD-6	**Validate the sponsor has recertified acknowledgement of responsibility for the digital worker at required intervals.**	N/A	✓ Verify sponsor recertification annually	✓ Verify sponsor recertification annually	✓ Verify sponsor recertification every six months
VD-7	**Validate the custodian has recertified acknowledgement of responsibility for the digital worker at required intervals.**	N/A	✓ Verify custodian recertification annually	✓ Verify custodian recertification annually	✓ Verify custodian recertification every six months

Key Point	SP-3 is a similar but separate activity than VD-6. In SP-3 the sponsor acknowledges their role and responsibilities initially and reacknowledges them every six months. VD-6 is validation of the acknowledgement. Perform each action together or separately, but they are tracked separately for flexibility.

Key Point	VD-3, VD-4, and VD-5 are validating the code, ethics, and bias reviews that have been conducted. It is up to the individual agencies to ensure a standard for conducting such reviews is followed. Agency representatives, such as the sponsor or custodian, should collaborate within a community of practice to capture best practices on how to perform the various reviews in Step 2.2.

Step 3: Provision Identity

Capture the appropriate digital worker data elements. These attributes are stored in the agency IDMS or other systems.

3.1 Capture and Store Identity Management Data Elements

Identity management system data elements are identification and sponsorship elements. They include information to uniquely identify a digital worker or whom to contact for more details. Agencies usually store Identity management data elements in an identity management system or directory and should be required for any digital worker with a unique identity regardless of adverse impact level. Table 9 provides guidance and recommended data fields to capture the necessary digital worker identity elements.

Table 9. IDMS Data Fields

Identity Management System Data Fields (DF)			
ID	**IDMS Field Name**	**Field Type**	**Additional guidance**
DF-1	**Digital Worker** *(new field)*	Boolean *e.g., Checkbox, True/False, yes/no, etc.*	*Denote if this is (Yes/True) or is not (No/False) a digital worker.*
DF-2	**Agency unique user ID** *(existing field)*	Text *Recommend using "DW" or other uniqueness element followed by the identifier based on agency naming conventions*	*Use a distinguishing and standard naming convention for digital workers. This isn't a card holder unique identifier (CHUID) or related to PIV.*
DF-3	**First Name** and **Last Name** *(existing fields)*	Text ***First name:*** *group function* ***Last name:*** *"DW" followed by a numerical value*	*Use agency naming convention if IDMS requires first and last name. The first name field should be completed with the group function (e.g., Technology Division, CFO) and the last name field should be completed with "DW" followed by*

			a numerical value corresponding with the sequential order in which the digital worker was built within the associated group function.
DF-4	**Digital Worker Sponsor Name** *(new field[s])*	Text *Recommend the individual's full name (generally first and last name)*	*Specify the sponsor of the digital worker.*
DF-5	**Digital Worker Custodian Name** *(new field[s])*	Text *Recommend the individual's full name (generally first and last name)*	*Specify the custodian of the digital worker.*
DF-6	**Digital Worker Description** *(optional new field)*	Text (250) *Recommend including a brief description of the digital worker (e.g., the type of AI used, the purpose, and actions of the digital worker)*	*Provide a short description of what the digital worker does, and the type of digital technology used.*
DF-7	**Responsible Organization** *(optional new field)*	Text *Include the name of the organization according to the official agency organizational chart*	*Specify the name of the responsible agency organization or group.*

3.2 Capture and Store Identity Governance Data Elements

Identity governance data elements validate and recertify access. They include information used to report on digital worker access and include information on:

- Acknowledgment date;
- Recertification date;
- Adverse impact level; and
- Other completion or acknowledgment dates.

Agencies may store and track identity governance data elements in an existing system like an identity governance or directory management tool. The agency should develop an appropriate method or process to track these elements if one doesn't exist.

Table 10. Identity Governance Data Elements

Identity Governance Data Elements		
ID	**Data Element**	**Additional Guidance**
DF-8	**Digital Worker Sponsor Date of Last Acknowledgement**	*Specify the date the sponsor acknowledged responsibility for the digital worker. Recommend including the date in the format specified by agency guidelines (e.g., 01/01/2020).*
DF-9	**Digital Worker Date of Sponsor Acknowledgement Recertification** *(optional)*	*Track when the sponsor acknowledgement must be recertified. This can be tracked as a formula based on the last acknowledgement date and adverse impact level requirements, or a format and method specified by agency guidelines.*
DF-10	**Level of Potential Adverse Impact**	*Specify the level of potential adverse impact as determined using the methodology in section 3.2 of this document. Limited response (e.g., "Low", "Moderate," "High," or "Critical").*
DF-11	**Digital Worker Date of Last Custodian Acknowledgement**	*Specify the date the custodian acknowledged responsibility for the digital worker. Recommend including the date in the format specified by agency guidelines (e.g., 01/01/2020).*
DF-12	**Digital Worker Date of Custodian Acknowledgement Recertification** *(optional)*	*Track when the custodian acknowledgement must be recertified. This can be tracked as a formula based on the last acknowledgement date and adverse impact level requirements, or a format and method specified by agency guidelines.*

DF-13	**Approved Source Internet Protocol (IP) Address Range** *(only for High and Critical)*	*Specify the range of source IP addresses on which the digital worker may operate.*
DF-14	**Code Review Completion Date** *(optional)*	*Specify the code review completion date (refer to VD-3 for more details). Recommend including the date in the format specified by agency guidelines (e.g., 01/01/2020).*
DF-15	**Ethics Review Completion Date**	*Specify the digital worker ethics review completion date (refer to VD-4 for more details). Recommend including the date in the format specified by agency guidelines (e.g., 01/01/2020).*
DF-16	**Next Ethics Review Date** *(optional)*	*Track when the next ethics review date must be conducted. This can be tracked as a formula based on the last ethics review date and adverse impact level requirements, or a format and method specified by agency guidelines.*
DF-17	**Digital Worker Bias Review Completion Date**	*Specify the digital worker bias review completion date (refer to VD-5 for more details). Recommend including the date in the format specified by agency guidelines (e.g., 01/01/2020).*
DF-18	**Next Bias Review Date** *(optional)*	*Track when the next bias review date must be conducted. This can be tracked as a formula based on the last bias review date and adverse impact level requirements, or a format and method specified by agency guidelines.*

Conclusion

Digital worker identity management requires new government-wide policies and guidance tailored to digital workers' unique functional and security considerations. Government-wide adoption and implementation of this playbook provide agencies distinct actions on how to manage and maintain their digital workforce.

- **Step 1**: The Digital Worker Impact Evaluation Matrix helps agencies determine whether to establish an identity for a digital worker based on its potential level of adverse impact.
- **Step 2**: New sponsorship and validation processes establish digital worker accountability and confirms it will only act as programmed.
- **Step 3**: New identity management and identity governance data elements support an agency's ability to manage and monitor through the identity lifecycle.

This playbook is iterative, and agencies are encouraged to collaborate, share best practices, and lessons learned. Consider joining a federal committee and community of practice to learn and engage in digital worker identity management.

Appendix A: Digital Worker Impact Evaluation Factors

This section provides a detailed breakdown of the information contained in Table 2, the Digital Worker Impact Evaluation Matrix.

Factor 1 – Is the digital worker attended or unattended?
This factor assesses whether the digital worker is attended and overseen by a human worker in completing its operations.

Table 11. Factor 1 Criteria Details

Criteria	Details	Score
1a) Attended	An attended digital worker operates under constant supervision and attendance by a human, likely operating on the user interface level (e.g., either on the user's computer desktop or a separate computer attended by the human, typically acting on behalf of a human user).	**0**
1b) Unattended	An unattended digital worker doesn't operate under supervision or attendance by a human. A human doesn't oversee the direct action of the digital worker technology. The tool operates out of sight, including (but not limited to) on a virtual machine, through API calls, etc.	**10**

Factor 2 – What type of data does the digital worker access?
This factor assesses the impact-based sensitivity of data accessed by the digital worker to determine the potential adverse impact related to unauthorized disclosure of information and changing or destruction of information.

Table 12. Factor 2 Criteria Details

Criteria	Details	Score
2a) Data available to the public (either without a user account or with unvetted user account)	The digital worker only works with/has access to data that's fully available for use and access by the general public. It includes all information available on public forums (open websites and networks) and all information that the public may access through the setup of unvetted user accounts (e.g., a citizen can use an unvetted account to access Centers for Disease Control "public" data).	**0**
2b) Agency operational data, CUI, or data on individuals (no PII) in low volumes	The digital worker works with/has access to data that isn't for public consumption, including CUI, intellectual property owned by the government or outside organizations, and information related to agency operations.	**5**
2c) PII and PHI	The digital worker works with/has access to public data, agency operational data, and PII or PHI. This is a "trigger" criterion, meaning if the digital worker	**55**

Criteria	Details	Score
	meets this criterion, it automatically should be in at least a High potential adverse impact level according to the scale in Table 1.	
2d) Agency critical operational data or data that could impact life, health, or safety of individuals/systems relied upon for health and safety; or very high volumes of agency operational data	The digital worker works with/has access to data that could have catastrophic effects if made public, such as information about mission-critical agency operations, or information that impacts the life, health, and safety of individuals. This is a "trigger" criterion, meaning if the digital worker meets this criterion, it automatically should be in a Critical potential adverse impact level according to the scale in Table 1.	**90**

Factor 3 – Does the digital worker have access to internal and/or external networks?

This factor assesses what type of networks the digital worker accesses. There are different levels of potential impact depending on whether access is granted to internal networks, external networks, or both.

Table 13. Factor 3 Criteria Details

Criteria	Details	Score
3a) No internal intranet or external internet connection	The digital worker doesn't have access to any internal or external networks.	**0**
3b) Either internal intranet access only OR external internet access (but not both)	The digital worker only has access to internal networks and operates fully inside the agency's firewall; the digital worker only has access to external networks, operating outside the firewall.	**5**
3c) Internal and external network access (i.e., internet and intranet)	The digital worker has access to both internal networks and external networks (i.e, can cross the agency's firewall).	**10**

Factor 4 – What is the impact of the output generated by the digital worker?

This factor assesses the potential worst-case scenario impact of the output the digital worker generates on different stakeholder groups: internal organizational impact; external organizational impact; and critical, pervasive impacts across organizations, government, or society.

Table 14. Factor 4 Criteria Details

Criteria	Details	Score
4a) Output impacts general internal business operations, but not for critical processes or decisions	The output of the digital worker is used solely for and/or may impact internal organizational business processes, operations, and decisions. However, the output isn't used in critical organizational processes; if it is, then this would fall under criterion 4c.	**5**
4b) Output impacts outside organizations in general business operations or public reporting, but not for critical processes or decisions	The output of the digital worker is used for and/or may impact external organizational business processes, operations, and decisions. Additionally, the output may be used in public reporting GAO audits. However, the output shouldn't be used in critical organizational processes; if it is, then this would fall under criterion 4c.	**25**
4c) Output impacts mission critical organization operations of the agency or other organizations, health or safety of individuals, national economic stability, national security, critical infrastructure, or similarly consequential operations	The output of the digital worker is used for and/or may impact: mission critical operations of an organization, health and safety of individuals, national economic stability, national security, critical national infrastructure, or other similarly consequential operations. This is a "trigger" criterion, meaning if the digital worker meets this criteria, it automatically should be in a Critical potential adverse impact level according to the scale in Table 1.	**90**

Factor 5 – What type of system account privileges does the digital worker require?
This factor assesses the type and level of system account access that the digital worker requires to complete its tasks. Privileged access, especially for multiple systems, creates higher potential adverse impact than standard user accounts or no account use at all.

Table 15. Factor 5 Criteria Details

Criteria	Details	Score

5a) No system accounts used	The digital worker doesn't have any system accounts that are used to access databases, web applications, etc.	**0**
5b) Standard system account(s) (Roles limited by the business function)	The digital worker uses one or more system accounts that have a login (e.g., username, password, multi-factor authentication) to access databases, web applications, etc. The user privileges within the system account(s) are standard business user roles and have no system administrator privileges. The standard user roles are defined by the agencies and may include any combination of the following: read, write, execute, and delete.	**10**
5c) System admin account (privileged access)	The technology uses one or more system accounts that have a login (e.g., username, password, multi-factor authentication) to access databases, web applications, etc. Select this criterion if the digital worker will, or may need to have, access to systems or web applications with admin or otherwise, privileged access. If there are multiple system or web application accounts used by a technology, then only one may be admin or privileged access, as defined by the agency, and may include any combination of the following: read, write, execute, and delete. This is a "trigger" criterion, meaning if the digital worker meets this criterion, it automatically should be in at least a Moderate potential adverse impact level according to the scale in Table 1.	**35**
5d) Multiple system admin accounts (multiple privileged access roles)	The digital worker uses one or more system accounts that have a login (e.g., username, password, multi-factor authentication) to access databases, web applications, etc. Select this criterion if the digital worker will, or may need to have, access to systems or web applications with admin or some sort of privileged access. Additionally, select this criterion if the digital worker requires, or may in the future require, admin or privileged access to multiple systems or web applications, as defined by the agency, and may include any combination of the following: read, write, execute, and delete. This is a "trigger" criterion, meaning if the digital worker meets this criterion, it automatically should be in at least a Moderate potential adverse impact level according to the scale in Table 1.	**40**

Factor 6 – Does the digital worker act on its own insights?
This factor assesses the extent to which a human is involved in approving the decisions of digital workers. Digital workers that generate insights and then use those insights to make

decisions or complete actions are seen as having a greater potential adverse impact compared to digital workers that only generate insights or that generate insights but have a human review before completing a subsequent action.

Table 16. Factor 6 Criteria Details

Criteria	Details	Score
6a) Digital worker develops insights, but does not take action on its insights	The digital worker develops insights but doesn't take separate action based on the insights. (e.g., a digital worker is used to diagnose a patient based on medical history data fed to a machine learning algorithm, then the digital worker only provides a diagnosis recommendation and doesn't take any additional actions.)	**0**
6b) Digital worker develops insights and acts on the insights after human review	The digital worker is used first to develop insights. A human then reviews the insight and either edits or approves the insight. (e.g., a digital worker is used to diagnose a patient based on medical history data, then the tool will use the data to develop a diagnosis and recommended treatment [insight]. The doctor will review the diagnosis and recommended treatment. If the doctor disagrees with the insight, they will amend it; if the doctor agrees, they will approve it. Then, the digital worker administers the treatment to the patient.)	**5**
6c) Digital worker develops insights and acts on the insights without human review or approval before the action is taken	The tool develops insights and then uses the insight to determine a course of action. The tool proceeds with this action without human review of the initial insight. (e.g., a digital worker recommends a diagnosis and treatment based on data from the patient's medical history.The digital worker acts on this recommendation by administering treatment to the patient without a doctor's intermediary review.)	**10**

Appendix B: Critical Case Study

A government hospital uses a digital worker to diagnose patients.

- The digital worker uses an unattended machine learning algorithm on internal networks.
- It works with the patient's medical history, diagnostic test results, and thousands of previous patient outcome data sets containing PHI
- The digital worker develops a diagnosis and recommends a treatment.
- The digital worker uses only a standard user account during its tasks.

Table 17. Critical Case Study Digital Worker Impact Evaluation Matrix

Digital Worker Impact Evaluation Matrix	
Factor 1 - Is the digital worker attended or unattended?	**Score**
● Unattended	**10**
Factor 2 - What is the highest level of sensitive data access?	
● PII and/or PHI	**55**
Factor 3 - Does the digital worker have network access?	
● Either internal intranet access only OR external internet access (not both)	**5**
Factor 4 - What is the impact of the digital worker output?	
● Output impacts mission critical organization operations of the agency or other organizations, health or safety of individuals, national economic stability, national security, critical infrastructure, or similarly consequential operations	**90**
Factor 5 - What system account privileges are required to perform the task?	
● Standard system account(s) (roles limited by the business function)	**10**
Factor 6 - Does the digital worker act on its own insights?	
● Digital worker develops insights, but does not take action on its insights	**0**
Total Score	**170**
Digital Worker Adverse Impact Level	**Critical**

This digital worker impact level is Critical. It has the potential to cause severe or catastrophic impact. The overarching risk in this case study is the digital worker

recommendation impacting an individual's health and safety and access to PHI.

The hospital digital worker in this case study has a **critical** adverse impact level. We follow the below activities to assign a sponsor and custodian and validate the digital worker access and process.

Table 18. Critical Case Study Sponsorship and Validation

ID	Critical Actions
Hospital Digital Worker Sponsorship (SP)	
SP-1	The business owner documents the business need to use a digital worker.
SP-2	The CISO reviews the business need and assigns the systems Information Security System Manager (ISSM) as sponsor. The CISO notifies the ISSM and the ISSM electronically signs an acknowledgement letter every six months.
SP-3	
SP-4	As sponsor, the ISSM assigns and notifies the contractor maintaining the digital worker of their responsibility as custodian.
SP-5	
SP-6	The contractor, as custodian, acknowledges their assignment and responsibility every six months.
Hospital Digital Worker Validation (VD)	
VD-1	The ISSM, as sponsor, reviews the digital worker design document with the ISSO to verify a level of access that employs least privilege. They verify a standard system account is necessary.
VD-2	The ISSM and ISSO validate the standard system account does not create a separation of duty conflict with a human user.
VD-3	The ISSM verifies a code review was conducted with the business owner and sets a reminder to verify the code review every six months.
VD-4	The ISSM verifies with the ethics office that the digital worker output is in line with agency ethics and bias standards and sets a reminder to verify with the ethics office every six months.
VD-5	
VD-6	The ISSM and contractor, as sponsor and custodian, recertify acknowledgement of responsibility for the digital worker and sets a reminder to conduct this action every six months.
VD-7	

After the sponsorship and validation activities are complete and documented, the hospital digital worker identity was created and provisioned. Identity management data fields are

captured in the directory service. The identity governance data fields are captured in an agency security assessment tool.

Table 19. Critical Case Study Data Fields

Identity Management System Data Fields (DF)		
DF-1	**Digital Worker** *(new field)*	True
DF-2	**Agency unique user ID** *(existing field)*	Diagnosis.DW01@agency.gov
DF-3	**First Name** and **Last Name** *(existing fields)*	*Diagnosis DW01*
DF-4	**Digital Worker Sponsor Name** *(new field[s])*	Jane ISSM
DF-5	**Digital Worker Custodian Name** *(new field[s])*	Stacy Contractor
DF-6	**Digital Worker Description** *(optional new field)*	N/A
DF-7	**Responsible Organization** *(optional new field)*	Patient Health Division
Additional Identity Governance Data Fields		
DF-8	**DW Sponsor Acknowledgement Date**	09/1/2020
DF-9	**DW Sponsor Acknowledgement Recertification Date** *(optional)*	02/1/2021
DF-10	**DW Level of Potential Adverse Impact**	Critical
DF-11	**DW Custodian Acknowledgement Date**	09/10/2020
DF-12	**DW Custodian Acknowledgement Recertification Date** *(optional)*	02/10/2021
DF-13	**DW Approved Source Internet Protocol (IP) Address Range** *(only for High and Critical)*	192.168.0.0/16
DF-14	**DW Code Review Completion Date** *(optional)*	07/04/2020
DF-15	**DW Next Code Review Date** (optional)	01/04/2021
DF-16	**DW Ethics Review Completion Date**	07/11/2020
DF-17	**DW Next Ethics Review Date** *(optional)*	01/11/2021
DF-18	**DW Bias Review Completion Date**	07/11/2020
DF-19	**DW Next Bias Review Date** *(optional)*	01/11/2021

Appendix C: Low Case Study

A digital worker assists the General Services Administration gather data on COVID-19.

- The digital worker is unattended, uses a standard system account, and has internal and external network access.
- Pulls data from public state government websites to aggregate and populate a Geographic Information System map.
- The output isn't decision critical and provides insights with no actions.

Table 20. Low Case Study Digital Worker Impact Evaluation Matrix

Digital Worker Impact Evaluation Matrix	
Factor 1 - Is the digital worker attended or unattended?	**Score**
• Unattended	**10**
Factor 2 - What is the highest level of sensitive data access?	
• Data available to the public (either without a user account or with unvetted user account)	**0**
Factor 3 - Does the digital worker have network access?	
• Internal and external network access (i.e., internet and intranet)	**10**
Factor 4 - What is the impact of the digital worker output?	
• Output impacts general internal business operations, but not for critical processes or decisions	**5**
Factor 5 - What system account privileges are required to perform the task?	
• Standard system account(s) (roles limited by the business function)	**10**
Factor 6 - Does the digital worker act on its own insights?	
• Digital worker develops insights, but does not take action on its insights	**0**
Total Score	**35**
Digital Worker Adverse Impact Level	**Low**

This digital worker impact level is Low. It's effect of an error or accident is minimal, resulting in negligible impacts. Low does not require a unique identity for a digital worker. The impact level is documented and a reminder is set to reassess the impact level with any code change.