National Security Agency | Cybersecurity Information

Selecting Secure Multi-factor Authentication Solutions

United States Government Agencies are required by the Federal Information System Management Act (FISMA) to utilize Personal Identity Verification (PIV) cards to authenticate employees to official information systems. During a global pandemic or in other scenarios where authorized users do not have access to government furnished equipment (GFE) or cannot utilize a PIV card, using other strong authentication mechanisms becomes necessary and unavoidable.[1, 2]

U.S. Government Agencies and their partners who want to integrate secure alternatives to PIV-based authentication need to support authorized users who will be employing personally owned or partner-owned devices, such as smart phones and home or non-government office computers, to access government or partner information systems containing sensitive information. By using the objective criteria in this guidance, government organizations can make better informed decisions about which multi-factor solutions meet their particular needs. And by following the practical guidelines, users can reduce their risk exposure and become harder targets for malicious threat actors.[3]

Criteria to consider when selecting a multi-factor authentication solution

The National Institute of Standards and Technology's Computer Security Resource Center recently updated its "Digital Identity Guidelines[4]" (SP 800-63-3). It provides standard definitions and assigns assurance levels for various authentication solutions. The criteria below reflect NIST's requirements to ensure that a solution is validated to resist a number of common exploits.

A complete authentication solution must be properly implemented using standard, validated mechanisms. It must also include authenticators, validators, and supporting lifecycle processes. Some commercial solutions focus on authenticators and require an organization to manage validators and lifecycle processes. Other commercial solutions validate multiple types of authenticators, manage multi-step authentication mechanisms, and manage trust in authenticators from various identity providers in support of multiple services. These often require the customer to acquire one or more authenticator solutions and configure servers to accept the assertions of an authentication server that performs identity federation. SP 800-63-3 also includes criteria for identity federation.

NIST's "Digital Identity Guidelines" consists of the following three parts:

- **SP 800-63-3 Part A** defines identity vetting processes that are expected to be managed by the organization as part of their identity lifecycle management. Part A is not covered in this document.
- **SP 800-63-3 Part B** defines three authenticator assurance levels (AAL) for authenticators. Government Agencies require AAL 2 solutions for access to official information systems, and may require AAL 3 solutions for access to sensitive or mission critical information; solutions that do not align to SP 800-63-3, or which only provide AAL 1 mechanisms, are not discussed in this document.
- **SP 800-63 Part C** discusses identity federation and defines three Federation Assurance Levels (FAL).

To provide a complete and secure authentication solution for your organization, evaluate possible solutions against the following criteria:

1. **Does the solution adequately protect the authenticator from common exploitation techniques?** Most authentication solutions depend on secret keys that require integrity protection, protection from disclosure, and properly implemented secure random number generators and cryptography.

[1] This is also true for collaboration scenarios where some authorized users cannot obtain a PIV card.
[2] For more information, please refer to "Transition to Multi-factor Authentication," part of NSA's *Cybersecurity Top Ten Mitigations.*
[3] Individual departments and agencies may provide specific services or issue specific direction for their teleworkers. This document does not override or supersede any official guidance provided by your organization. Consult your department or agency IT support or CIO organization for further guidance.
[4] See csrc.nist.gov/publications/detail/sp/800-63/3/final

2. **Does the solution ensure the validator is effective in confirming that a request for access is from the user bound to the authenticator?** Confirming this binding requires proof-of-possession of ‘what you have’ and evidence that ‘what you know’ and/or ‘what you are’ have been confirmed.

3. **Are communications among components of the authentication solution adequately protected using strong, well-known, and testable cryptographic standards?** Communications need integrity protection, source authentication, and/or encryption to protect authentication evidence from modification or replay.

4. **Does the solution provide support for managing the lifecycle of digital identities and authenticators?** Organizations are responsible for the lifecycle management of digital identities. Solutions that support these activities can be more easily managed, and therefore often more securely managed.

5. **If the solution authenticates a user’s request on behalf of a requested service, does the solution securely communicate that authentication to the requested service?** Secure integration of an authentication solution into existing mechanisms ensures that the solution does not allow malicious actors to bypass authentication.

The detailed criteria used to answer these questions depend on the type of multi-factor authentication mechanism used. SP 800-63-3 defines a number of single response multi-factor mechanisms, as well as combinations of single-factor mechanisms (referred to as multi-step authentication mechanisms) suitable for AAL 2 or AAL 3. The authenticator type can be implemented in a hardware device (e.g., a key-chain fob) or by software installed on a mobile device.

Single response, multi-factor authentication mechanisms require activation of the device, either with a PIN/password or biometric. The device provides ‘what you have’ and activation of the device implies that ‘what-you-know’ or ‘what-you-are’ has been verified.

On the other hand, multi-step authenticators often include a password to provide ‘what-you-know’ and another authenticator that provides ‘what-you-have’. Note that SP 800-63-3 Part B defines the requirements for PIN/password activation differently from the passwords that are used directly to provide ‘what-you-know’. PINs/passwords used for activation of an authenticator device are typically 6-to-8 characters and the device integrates thresholds to address password guessing attacks, whereas passwords used directly are required to be longer and have complexity requirements.

Using multi-factor authentication services securely

If possible, use GFE that is managed and intended for government use only. No authentication mechanism can defend against a compromised device. Personal devices are often exposed to considerable risk of compromise due to failure to apply patches in a timely fashion or installing an application that users fail to recognize as being malicious. Resulting malware infections can interface with connected authenticators to initiate unauthorized accesses or replay a passcode input into the compromised device. This is true for PIV authentication as well as the alternative authentication mechanisms discussed in this document.

Carefully managed GFE devices are often more secure than personal devices, unless configuration control policies delay the deployment of critical patches. If GFE is available, it should be used. If GFE cannot be used, NSA recommends a temporary secure operating system such as the publicly-available DoD Trusted End Node Security (TENS) solution to create a “virtual GFE”.[5] If neither is practical, device owners should ensure that user accounts do not have administrator privileges (which are only for managing the system). If possible, device owners should also create a separate user account with low privileges for only work use.[6]

Ensure all components of the authentication solution are securely integrated. Integrating multi-factor authentication techniques into customer servers can be challenging. Even for PIV, it is important to pay attention to validator

[5] For more information about TENS, please see www.tens.af.mil/.
[6] For more information on protecting personal devices, please refer to NSA’s “Best Practices for Keeping Your Home Network Secure”.

configurations to ensure that the authentication mechanism is not easily bypassed. When configuring commercial multi-factor authentication solutions:

- Use only configurations that support approved authenticators.
- Ensure that all software components (client agents, authentication software, platform O/S, and validation software) are patched and up-to-date.
- Support the digital identity and authenticator specific lifecycle requirements.
- Monitor for unexpected or malicious behaviors.

Train all users on the proper handling of authenticators. Users must not disclose ‘what-you-know’ and maintain control of authenticators that convey ‘what-you-have’. In addition to understanding these responsibilities, users need to know how to report a potential compromise resulting from inadvertent loss of control of devices or authenticators.

Assessment of common multi-factor authentication solutions

The following table, based on publicly available information, illustrates how various common solutions claim to meet the SP 800-63-3 criteria for the types of mechanisms supported. The list below includes common solutions that completed Federal Information Processing Standard (FIPS) validation within the last 2 years as well as those non-FIPS-validated solutions with current DoD approvals. Where the authenticator or validator is FIPS 140-2 validated, the certificate number is listed. On-premises implementations of the validator require NIST SP 800-53 moderate baseline security controls for AAL 2, and high baseline controls for AAL 3, as noted in the validator column – other dependencies are listed specifically. Partial AAL compliance refers to solutions where evidence of compliance is lacking – with the specific requirement that is needed noted. Since the criteria depend on the specific type of authenticator, this is denoted in the ‘Type’ column of the table using the following key:

Key:	Authentication method	Multi-factor authenticator	Form factor
	Out-of-Band (OOB)	Multi-factor - PIN/password or Biometric Activation (MF)	Device (D)
	One-Time Password (OTP)	Single factor - Activation Not Required (SF)	Software (SW)
	Cryptographic Signature (Crypt)		
	Direct Password (PW)		

Table I: Examples of Multi-factor Authentication Solutions - alternatives to PIV

Solution	Type and AAL	Authenticator	Validator	Secure channel	Lifecycle support	Federation
Duo Federal MFA[7]: Duo Mobile Passcode	PW (provided by client, server) + SF-OTP-SW AAL 2 – dependent on client, server	FIPS validated (#2671) Duo Mobile Passcode SW installed on: • iOS 6+ • Android 3.25+ • Windows Phone 2.0+	FEDRAMP[8] approved Depends on compliant native logon	TLS 1.2 HTTPS (StartTLS), LDAPS Native logon uses RDP	Device and User Enrollment Authenticator Revocation	Authentication Agent and Proxy integrate with FIPS validated Windows®[9]: or Linux®[10] OS

[7] Refer to “Cisco’s® Duo Security Achieves FedRAMP Authorization” (blogs.cisco.com/government/fedramp-authorization-cisco-duo-security) for vendor claims. Refer to “Guide to Duo’s Federal Editions” (duo.com/docs/duo-federal-guide) for guidance and dependency information. Cisco® is a registered trademark of Cisco Systems, Inc..
[8] Refer to fedramp.gov/assets/documents/CSP_Digital_Identity_requirements.pdf for SP 800-63-3 B AAL 2 compliance.
[9] Windows® is a registered trademark of Microsoft Corporation.
[10] Linux OS® is a registered trademark of Linus Torvalds.

Solution	Type and AAL	Authenticator	Validator	Secure channel	Lifecycle support	Federation
Duo Federal MFA[11]: Duo Mobile Push	PW (provided by client, server) + SF-OOB-SW **AAL 2** – dependent on client, server	FIPS validated (#2671) Duo Mobile Push SW installed on: • iOS 6+®[12] • Android 3.25+®[13] • Windows Phone 2.0+®[14]	FEDRAMP[15] approved Depends on compliant native logon	TLS 1.2 HTTPS (StartTLS), LDAPS Native logon uses RDP	Device and User Enrollment Authenticator Revocation	Authentication Agent and Proxy integrate with FIPS validated Windows® or Linux® OS
Duo Federal MFA[16]: Third Party Token	PW (provided by client, server) + SF authenticator or MF authenticator **AAL 2** –dependent on token, client, server.	Requires FIPS validated token Supports: • Yubikey OTP®[17] • WebAuthn Crypt Tokens	FEDRAMP[18] approved Use of PW dependent on compliant native logon	TLS 1.2 HTTPS (StartTLS), LDAPS Native logon uses RDP	Device and User Enrollment Authenticator Revocation	Authentication Agent and Proxy integrate with FIPS validated Windows® or Linux® OS
Google®[19] Authenticator	PW (provided by client, server) + SF-OTP **Partial AAL 2** – requires integration into FIPS validated platform; dependent on client, server, validator	Open source app requires integration into FIPS validated platform[20] Supports: • Android® • BlackBerry®[21] • iOS®	Requires compliant validator	Dependent on client, server using TLS 1.2	No information provided	Dependent on validator capabilities

[11] Refer to "Cisco's Duo Security Achieves FedRAMP Authorization (blogs.cisco.com/government/fedramp-authorization-cisco-duo-security) for vendor claims. Refer to "Guide to Duo's Federal Editions" (duo.com/docs/duo-federal-guide) for guidance and dependency information.

[12] iOS® is a registered trademark of Cisco Systems, Inc. in the United States and other countries and is used under license to Apple, Inc.

[13] Android® is a registered trademark of Google LLC.

[14] Windows Phone® is a registered trademark of Microsoft Corporation.

[15] Refer to fedramp.gov/assets/documents/CSP_Digital_Identity_requirements.pdf for SP 800-63-3 B AAL 2 compliance.

[16] Refer to "Cisco's® Duo Security Achieves FedRAMP Authorization (blogs.cisco.com/government/fedramp-authorization-cisco-duo-security) for vendor claims. Refer to "Guide to Duo's Federal Editions" (duo.com/docs/duo-federal-guide) for guidance and dependency information.

[17] Yubico® is a registered trademark of Yubico or Yubico's Licensors.

[18] Refer to fedramp.gov/assets/documents/CSP_Digital_Identity_requirements.pdf for SP 800-63-3 B AAL 2 compliance.

[19] Google® is a registered trademark of Google, Inc.

[20] Refer to github.com/google/google-authenticator/wiki. No FIPS 140-2 claims for current proprietary implementations.

[21] BlackBerry® is a registered trademark of BlackBerry.

Solution	Type and AAL	Authenticator	Validator	Secure channel	Lifecycle support	Federation
Microsoft® Authenticator	PW + SF-OTP **Partial AAL 2** – requires integration of SW into FIPS validated platform.	Not FIPS validated[22] Supports: • Android® • iOS® • Win 10 Mobile®[23] • Windows Phone® 8.0, 8.1	Government cloud services FEDRAMP approved[24]	TLS 1.2 supported	Guidance provided for administrators	Integrated into Azure®[25] AD®[26]
Microsoft Azure® Multi-factor[27]: Third Party OATH HW Token	PW + SF/MF-OTP or **AAL 2/3** –dependent on token	Requires FIPS validated token	Government cloud services FEDRAMP approved[28]	TLS 1.2 supported	Guidance provided for adminstrators	Integrated into Azure® AD®
OKTA®[29] Verify (FIPS 140-2 validated option)[30]	PW + SF-OTP **AAL 2** – dependent on validator	FIPS validated (#3344) SW installed on: • iOS® 7+ • Android® 6+	FIPS validated crypto (#3344) Dependent on SP 800-53 controls	Enforces TLS 1.2	Device and User Enrollment Post Enrollment (to add additional authenticators) Authenticator Expiration and Revocation	Integrates with FIPS validated Windows®
OKTA® Third party OTP HW	PW + SF/MF-OTP **AAL 2** – token, validator dependent	Requires FIPS validated token Supports: • Google® Authenticator • Duo Mobile Passcode • RSA®[31] SecurID • WebAuthn token • Yubikey® OTP	FIPS validated crypto (#3344) for OTP Dependent on SP 800-53 controls	Enforces TLS 1.2	Device and User Enrollment Post Enrollment (to add additional authenticators) Authenticator Expiration and Revocation	Integrates with FIPS validated Windows®

[22] Beraud, P. Jumelet, A., & Grasse, J. (2015) “Leverage Azure Multi-Factor Authentication with Azure® AD® – Microsoft®” (pp. 1-40, Rep). Microsoft® France

[23] Windows® is a registered trademark of Microsoft Corporation in the United States and/or other countries.

[24] Refer to docs.microsoft.com/en-us/Microsoft-365/compliance/offering-fedramp?view=o365-worldwide. Compliant with FedRamp High controls (SP 800-53, SP 800-63B AAL 3).

[25] Azure® is a registered trademark of Microsoft Corporation in the United States and/or other countries.

[26] Active Directory (AD)® is a registered trademark of Microsoft Corporation in the United States and/or other countries.

[27] Refer to docs.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-howitworks. Supports OATH compliant tokens.

[28] Refer to docs.microsoft.com/en-us/Microsoft-365/compliance/offering-fedramp?view=o365-worldwide.. Compliant with FedRamp High controls. Refer to fedramp.gov/assets/resources/documents/CSP_Digital_Identity_requirement.pdf for SP 800-63-3B AAL 3 compliance.

[29] OKTA® is a registered trademark of Okta, Inc.

[30] Refer to www.okta.com/blog/2019/01/okta-releases-fips-140-2-validated-encryption-in-okta-verify for details about Okta’s® FIPS 140-2 claims.

[31] RSA® is a registered trademark of RSA Security LLC.

Solution	Type and AAL	Authenticator	Validator	Secure channel	Lifecycle support	Federation
OneLogin™[32] Protect[33]	PW + OTP **Partial AAL 2** – requires authenticator integration into FIPS validated platform, and additional validator controls.	No FIPS 140-2 validation. Solutions for: • iOS® • Android®	AICPA SOC compliant[34] No FIPS 140-2 validated crypto	No specific reference to traffic protection	No details indicated	SAML, OpenAuth Webauthn assertions
OneLogin™ PKI Browser Certificate[35]	PW + SF-Crypt-SW **Partial AAL 2** – requires additional validator controls; dependent on client.	Dependent on integration into FIPS validated client browser or OS	AICPA SOC compliant[36] No FIPS 140-2 validated crypto	No specific reference to traffic protection	No details indicated	SAML, OpenAuth Webauthn assertions
OneLogin™, Third party token	Third party token **Partial AAL 2** – requires additional validator controls, FIPS; dependent on token	Requires FIPS validated token Supports: • Duo®[37] Mobile Push • Google® Authenticator • Google Titan™[38] • RSE SecurID®[39] • YubiKey® • WebAuthn	AICPA SOC compliant[40] No FIPS 140-2 validated crypto	No specific reference to traffic protection	No details indicated	SAML, OpenAuth Webauthn assertions

[32] Onelogin™ is a registered trademark of Onelogin.

[33] Refer to onelogin.com/kb_view_customer.do?sysparm_article=KB0010426, for a general description, as well as onelogin.com/kb_view_customer.do?sysparm_article=KB0010517 (iOS), and onelogin.com/kb_view_customer.do?sysparm_article=KB001011 (Android®) for information regarding the solution's implementation for a particular device type.

[34] Refer to onelogin.com/compliance: OneLogin® claims compliance with AICPA, ISO, and CSA STAR, none of which fully address SP-800-53 baselines (refer to aicpa.org/interestareas/frc/assuranceadvisoryservices/aicpacybersecurityinitiative.html for comparison). OneLogin® also claims security controls are aligned with SP 800-53, but with no claims for compliance to baselines.

[35] Refer to onelogin.com/kb_view_customer.do?sysparm_article=KB0010604. Only supports OneLogin® certificates; Certification authority (part of validator function) is not NIAP validated.

[36] Refer to onelogin.com/compliance: OneLogin® claims compliance with AICPA, ISO, and CSA STAR, none of which fully address SP-800-53 baselines (refer to aicpa.org/interestareas/frc/assuranceadvisoryservices/aicpacybersecurityinitiative.html for comparison). OneLogin® also claims security controls are aligned with SP 800-53, but with no claims for compliance to baselines.

[37] Duo® is a registered trademark of Duo Security, Inc.

[38] Google Titan™ is a registered trademark of Google, Inc.

[39] RSE® is a registered trademark of EMC Corporation in the United States and/or other countries.

[40] Refer to onelogin.com/compliance: OneLogin® claims compliance with AICPA, ISO, and CSA STAR, none of which fully address SP-800-53 baselines (refer to aicpa.org/interestareas/frc/assuranceadvisoryservices/aicpacybersecurityinitiative.html for comparison). OneLogin® also claims security controls are aligned with SP 800-53, but with no claims for compliance to baselines.

Solution	Type and AAL	Authenticator	Validator	Secure channel	Lifecycle support	Federation
RSA SecurID®[41] SID 800 HW	MF-OTP **Partial AAL 2** – requires FIPS validated token or integration into FIPS validated platform; dependent on validator controls	Partial FIPS 140-2 validation[42] (#844) Approved for DoD	Authentication manager v8.2+ FIPS 140-2 validated (#3184) Dependent on SP 800-53 controls	Compliant TLS 1.2	Token management support	Agent integrates with FIPS validated Windows® or Linux® OS; SAML assertions
RSA SecurID® SID 700 HW	MF-OTP **Partial AAL 2** – requires FIPS validated token ; dependent on validator controls	Not FIPS 140-2 validated[43] Approved for DoD	Authentication manager v8.2+ FIPS 140-2 Validated (#3184) Dependent on SP 800-53 controls	Compliant TLS 1.2	Token management support	Agent integrates with FIPS validated Windows® or Linux® OS
RSA SecurID® SW tokens	MF-OTP **AAL 2** – dependent on validator controls	SW installed on FIPS validated device: • iOS® 2.4.6 - 2.4.8 (#3172) • Android® 2.4 -2.71 (#2097)	Authentication manager v8.2+ FIPS 140-2 Validated (#3184) Dependent on SP 800-53 controls	Compliant TLS 1.2	Token management support	Agent integrates with FIPS validated Windows or Linux® OS
Yubikey® OTP (touch)[44]	PW (Provided by client, server) + SF-OTP-D **Partial AAL 2** – requires compliant validator; dependent on client, server	FIPS validated (#3517) Approved for DoD	Requires compliant validator	Dependent on client, server use of TLS 1.2	Token management support	Dependent on validator cabilities

[41] RSA® is a registered trademark of EMC Corporation in the United States and/or other countries.

[42] Refer to community.rsa.com/docs/DOC-46887: SID 800 in FIPS mode uses a FIPS validated chip and OS

[43] Refer to community.rsa.com/docs/DOC-46887: SID 700 is not FIPS validated.

[44] Refer to www.yubico.com/solutions/cybersecurity-compliance. Yubikey® in OTP mode and configured for touch activation is an authenticator that can interface with a SP 800-63-3 AAL 2 compliant validator and an existing password-based logon, to create an AAL 2 compliant solution.

Solution	Type and AAL	Authenticator	Validator	Secure channel	Lifecycle support	Federation
Yubikey® U2F (touch)[45]	PW (Provided by client, server) + SF-Crypt-D **Partial AAL 2** – requires compliant validator; dependent on client, server	FIPS validated (#3517) Approved for DoD	Requires compliant validator	Dependent on client, server use of TLS 1.2	Token management support	Dependent on validator capabilities
Yubikey® OTP (fingerprint, PIN)[46]	MF-OTP-D **Partial AAL 2** – requires compliant validator; dependent on client, server	FIPS validated (#3517) Approved for DoD	Requires compliant validator	Dependent on client, server use of TLS 1.2	Token management support	Dependent on validator capabilities
Yubikey® (U2F/PIV)	MF-Crypto-D **Partial AAL 3** – requires compliant validator; dependent on client, server.	FIPS validated (#3517) Approved for DoD	Requires compliant validator	Dependent on client, server use of TLS 1.2 with client authentication	Token management support	Dependent on validator capabilities

Some commercial solutions support additional multi-factor authentication methods not defined in SP 800-63-3 for AAL 2 or 3. While such solutions might arguably provide better authentication than username/password alone, it is not clear that all desired features are provided. For example, SMS authentication (OOB) is not recommended without mitigations because it is fairly simple to redirect SMS messaging and defeat the ‘what you have’ factor. Also, biometric authentication for uses other than activation of a user device is not recommended. The majority of biometric solutions used in a user authentication setting do not have independent certification of accuracy or security. Examples of programs providing independent verification of biometric solutions include those associated with FIPS 201 (PIV) systems[47], and an emerging effort associated with the FIDO Alliance[48]. Similarly, combinations of single-factor authenticators not identified in SP 800-63-3 in support of AAL 2 or AAL 3 might not combine effectively to meet the desired strength. This document does not address vendor claims that are inconsistent with SP 800-63-3.

[45] Refer to www.yubico.com/solutions/cybersecurity-compliance. Yubikey®, in U2F mode and configured for touch activation is an authenticator that can interface with a SP 800-63-3 AAL 3 compliant validator and an existing password-based logon, to create an AAL 2 or AAL 3 compliant solution depending on the client and validator.

[46] Refer to www.yubico.com/solutions/cybersecurity-compliance. Yubikey®, in U2F or PIV mode, configured for fingerprint or PIN activation, is an authenticator that can interface with a SP 800-63-3 AAL 3 compliant validator to create an AAL 3 compliant solution.

[47] Refer to idmanagement.gov/sell/fips201/

[48] Refer to fidoalliance.org/certification/biometric-component-certification.

Purpose

This document was developed in furtherance of NSA's cybersecurity missions, including its responsibilities to identify and disseminate threats to National Security Systems, Department of Defense, and Defense Industrial Base information systems and to develop and issue cybersecurity specifications and mitigations, as well as to assist Executive departments and agencies with operations security programs. This information may be shared broadly to reach all appropriate stakeholders.

Disclaimer of Endorsement

The information and opinions contained in this document are provided "as is" and without any warranties or guarantees. Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by the United States Government, and this guidance shall not be used for advertising or product endorsement purposes.

Note that this does not constitute a Qualified Products List, within the meaning of the definition of Federal Acquisition Regulation (FAR) 2.101 or a Qualified Manufacturers List under FAR subpart 9.2—Qualification Requirements. The government has not undertaken any testing or evaluation of the products listed under this analysis, but has only reviewed the published attributes of the products. The list is not all-inclusive. This list may be amended and supplemented from time to time as market research discloses other items or new products become available. The descriptions and procedures explained in this document do not constitute or imply an endorsement by NSA/CSS, DoD, or USG of the products in question. It is intended solely for the non-commercial use of USG personnel for purpose of explaining and giving operating instructions for the use of the particular product in question. Any further use for other purposes is prohibited.

Contact

Client Requirements / General Cybersecurity Inquiries: Cybersecurity Requirements Center, 410-854-4200, Cybersecurity_Requests@nsa.gov
Media inquiries / Press Desk: Media Relations, 443-634-0721, MediaRelations@nsa.gov