OMB Checklist Policy or Procedure	NIST Control Family	NIST Control	Policy Statement(s)	ADS Reference(s) / Annotation(s)
Verify that Agency policy addresses the protection requirements of personally identifiable information (including that which is accessed remotely or removed from the security perimeter).	AC	Agency policy for PII must address purpose, scope, roles, responsibilities, and compliance and facilitate the implementation of access policy and controls. (AC-1.1, AC-1.2, AC-1.4)		This is covered by multiple policy statements. (Reminder Notices)
		(AC-1.3)	The System Owner must document the logical access controls implemented for each USAID information system and evaluate the effectiveness of the logical access control during the certification of the information system.	545.3.3.2 paragraph c (addition)
		(AC-1.3)	The Chief Information Security Officer, as the Certifying Official for the USAID enterprise, must evaluate the certification of the USAID information system and must determine whether the risk is acceptable to the enterprise.	545.3.1.7 paragraph a (3) (addition)
		(AC-1.6)	The System Owner must apply the Federal logical access controls to each USAID information system, and must comply with Chief Information Security Officer standards for logical access controls.	545.3.3.2 paragraph b (addition)
		(AC-1.7)	The Chief Information Security Officer must annually evaluate the policy requirements for access controls and update them to comply with changes to public laws, directives, regulations, standards, and guidance.	545.3.3.2 paragraph e (addition)

Verify that the agency enforces the controls for access and downloading of personally identifiable information.	AC	Agency assigned authorizations in accordance with policy. (AC-3.1, AC-3.4)		545.3.2.1 paragraph a (1), 545.3.2.1 paragraph c (2) (Reminder Notices)
		(AC-3.2)		545.3.2.1 paragraph c (2) (Reminder Notice)
		(AC-3.3)	The System Owner must annually review the user logical access rights for each USAID information system and determine if the access rights are consistent with those stated in the System Security Plan for the information system.	545.3.3.2 paragraph d (addition)
		(AC-3.5)	The System Owner must document the logical access controls implemented for each USAID information system and evaluate the effectiveness of the logical access control during the certification of the information system.	545.3.3.2 paragraph c (addition)
		(AC-3.6)	The Chief Information Security Officer must annually evaluate the policy requirements for access controls and update them to comply with changes to public laws, directives, regulations, standards, and guidance.	545.3.3.2 paragraph e (addition)
		(AC-3.7)		545.3.2.7 paragraph a (4) (Reminder Notice)
		(AC-3.8)		545.3.2.1 paragraph a (1), 545.3.2.1 paragraph c (2) (Reminder Notices)
Verify that the agency enforces the controls for access and downloading of personally identifiable information.	AC	Agency enforces assigned authorizations/security controls for information flow. (AC-4.1, AC-4.3)	The Chief Information Security Officer must develop USAID-specific policy directives and required procedures for what high-level types of information are permitted to be transferred between systems, and for regulating information flow between systems.	545.3.2.14 paragraph c (addition)
		(AC-4.1, AC-4.3)	The System Owner must apply security controls for their system, as determined by the information type and security categorization, to restrict the flow of information within the system and between interconnected systems.	545.3.2.14 paragraph d (addition)

		(AC-4.1)	The System Owner must not authorize information transfers that contain personally identifiable information between systems without conducting privacy impact assessments and declaring the sharing of personally identifiable information.	545.3.2.14 paragraph f (addition)
		(AC-4.1)	The System Owner must not authorize information transfers between a system that is categorized at a higher level to a system that is categorized at a lower level or systems categorized at similar levels, without evaluation of the data to be transferred, evaluation of the security controls of the recipient system, and written waiver by the Chief Information Security Officer.	545.3.2.14 paragraph e (addition)
		(AC-4.5)	The Chief Information Security Officer must annually evaluate the policy requirements for information sharing and update them to comply with changes to public laws, directives, regulations, standards, and guidance.	545.3.2.14 paragraph g (addition)
Verify that the agency enforces the controls for access and downloading of personally identifiable information.	AC	Agency assigned authorizations in accordance with policy. (AC-6.1)		545.3.2.1 paragraph a (1), 545.3.2.1 paragraph c (2) (Reminder Notices)
		(AC-6.2)	The System Owner and System ISSO must establish security controls and procedures for their information systems to authorize both user- and task- (service) account access rights and privileges that correspond to the authorized permissions defined for the system.	545.3.2.1 paragraph c (4) (addition)
		(AC-6.5)	The System Owner must annually review the user logical access rights for each USAID information system and determine if the access rights are consistent with those stated in the System Security Plan for the information system.	545.3.3.2 paragraph d (addition)
		(AC-6.6)	The Chief Information Security Officer must annually evaluate the policy requirements for access controls and update them to comply with changes to public laws, directives, regulations, standards, and guidance.	545.3.3.2 paragraph e (addition)

Verify that the agency enforces the controls for access and downloading of personally identifiable information.	AC	Agency supervises and reviews the activities of users who enforce access controls. (AC-13.1, AC-13.4)	The System Owner and System ISSO must establish audit controls for the access controls and procedures for their information systems to determine that no unauthorized access rights and privileges have been assigned to both user- and task- (service) accounts.	545.3.2.1 paragraph c (5) (addition)
		(AC-13.2)	The System Owner and System ISSO must review audit data at least quarterly for access rights and privileges on their systems.	545.3.2.1 paragraph c (6) (addition)
		(AC-13.2)	The System Owner and System ISSO must report unauthorized access rights and privileges which have been assigned to user- and task- (service) accounts to the Chief Information Security Officer.	545.3.2.1 paragraph c (7) (addition)
		(AC-13.5, AC-13.6)	The Chief Information Security Officer must annually evaluate the policy requirements for audit controls and update them to comply with changes to public laws, directives, regulations, standards, and guidance.	545.3.2.1 paragraph c (8) (addition)
		(AC-13.7, AC-13.8, AC-13.9)	Where required by security categorization or system size, the System Owner and System ISSO must employ an automated mechanism to support the assignment of user- and task- (service) account access rights and privileges.	545.3.2.1 paragraph c (9) (addition)
Verify that the Agency is using VPN technologies with two-factor authentication and proper encryption for remote access to systems that contain personally identifiable information.	AC	Agency applies controls for all methods of remote access. (AC-17.1, AC-17.14, AC-17.6, AC-17.8)	System Owners must not use any virtual private network (VPN) technology to permit access to USAID systems that does not use two factor authentication using remote tokens (i.e. server based computing), and that does not meet the FIPS 140-2 requirements for encryption.	545.3.5.2 paragraph d (addition)

		(AC-17.10)	The System Owner and System ISSO, for all systems that permit remote access, must record the remote access activity in audit logs, and review the audit logs at least quarterly for anomalies.	545.3.5.1 paragraph d (addition)
		(AC-17.10)	The System Owner and System ISSO must configure a remote time out parameter which, after a 30 minute or less period of session inactivity, terminates the session.	545.3.5.1 paragraph e (addition)
		(AC-17.16, AC-17.2)	The Chief Information Security Officer must annually evaluate the remote access requirements update them to comply with changes to public laws, directives, regulations, standards, and guidance.	545.3.5.1 paragraph f (addition)
Verify that Agency policy addresses the protection requirements of personally identifiable information (including that which is accessed remotely or removed from the security perimeter).	AT	Agency developed, disseminates, conducts and reviews its security awareness and training policy regarding PII. (AT-1.1, AT-1.2)	The Agency must establish and maintain a Privacy Awareness awareness program.	545.3.2.4 paragraph a (5) (addition)
		(AT-1.3, AT-1.7)	Staff must complete and maintain their annual privacy training and awareness, using the Agency-established programs, or be subject to the revokation of their access to Privacy Act-protected information.	545.3.2.4 paragraph a (8) (addition)
		(AT-1.3, AT-1.7)	The Agency must annually evaluate the effectiveness of its Privacy Awareness awareness program.	545.3.2.4 paragraph a (6) (addition)
		(AT-1.3)	The Agency must establish and provide annual Privacy Awareness training to all staff who use PII in routine performance of their jobs. For individuals who have additional responsibility for PII, the Agency must provide role-based training.	545.3.2.4 paragraph b (6) (addition)

		(AT-1.3, AT-1.7)	The Agency must annually evaluate the effectiveness of its Privacy Awareness training program.	545.3.2.4 paragraph b (7) (addition)
		(AT-1.5)	The Chief Privacy Officer must annually evaluate the requirements for the awareness program and update them to comply with changes to public laws, directives, regulations, standards, and guidance.	545.3.2.4 paragraph a (7) (addition)
		(AT-1.5)	The Chief Privacy Officer must annually evaluate the requirements for the training program and update them to comply with changes to public laws, directives, regulations, standards, and guidance.	545.3.2.4 paragraph b (8) (addition)
Verify that the Agency does not remotely store personally identifiable information.	AT	Agency initially trains all users (including managers and senior executives) before system access is granted and provides awareness materials at least annually thereafter. (AT-2.1, AT-2.2)		Security Tips of the Day (Reminder Notice)
		(AT-2.3)		545.3.2.4 paragraph a (Reminder Notice)
		(AT-2.4)	The Chief Information Security Officer must collect and retain the security training records for individuals who receive information security training.	
		(AT-2.5)	The Chief Information Security Officer must evaluate **annually** the security training program to determine its effectiveness, and change it if necessary.	545.3.2.4 paragraph b (3) (word-addition)

Verify that Agency policy addresses the protection requirements of personally identifiable information (including that which is accessed remotely or removed from the security perimeter).	AU	Agency develops, disseminates and updates its audit and accountability policies and procedures. (AU-1.1, AU-1.3, AU-1.4)	The System Owner and System ISSO must review audit data at least quarterly for access rights and privileges on their systems.	545.3.2.1 paragraph c (6), 545.3.5.1 paragraph (g) (addition)
		(AU-1.1, AU-1.7)	The Chief Information Security Officer must evaluate annually the baseline audit requirements for USAID information systems and if necessary make changes to them to comply with changes to public laws, directives, regulations, standards, and guidance.	545.3.5.1 paragraph h (addition)
		(AU-1.1, AU-1.2, AU-1.3, AU-1.4)	For all actual and suspicious incidents detected during audit reviews, the System Owner and System ISSO must immediately (within one hour) contact the Chief Privacy Officer and Chief Information Security Officer and must provide details of the incident sufficient that the Chief Information Security Officer can report the incident to the Office of Management and Budget and the Department of Homeland Security United States Computer Emergency Response Team (US-CERT) .	545.3.5.1 paragraph i (addition)
		(AU-1.1, AU-1.2, AU-1.3, AU-1.4)	For all actual and suspicious incidents detected, the System Owner and System ISSO must immediately (within one hour) contact the Chief Privacy Officer and Chief Information Security Officer and must provide details of the incident sufficient that the Chief Information Security Officer can report the incident to the Office of Management and Budget and the Department of Homeland Security United States Computer Emergency Response Team (US-CERT) .	545.3.2.3 paragraph e (addition)

		(AU-1.1, AU-1.3, AU-1.4)	The Chief Information Security Officer must report all actual and suspicious incidents reported to the Office of Management and Budget and the Department of Homeland Security United States Computer Emergency Response Team within one hour of being notified by the System Owner or System ISSO.	545.3.2.3 paragraph e (addition)
		(AU-1.1, AU-1.2, AU-1.3, AU-1.4)	The Chief Information Security Officer must notify the Administrator of all actual incidents reported to the Office of Management and Budget and the Department of Homeland Security United States Computer Emergency Response Team within one hour of being notified by the System Owner or System ISSO.	545.3.2.3 paragraph f (addition)
Verify that the agency enforces the controls for access and downloading of personally identifiable information.	AU	Agency information systems generate audit events. (AU-2.1, AU-2.3)	The System Owner and System ISSO must configure their system to record audit data.	545.3.5.1 paragraph g (addition)
		(AU-2.4)	The System Owner and System ISSO must retain their system audit records for periods defined by Federal public laws or regulations, or other period as defined by the Chief Information Security Officer.	545.3.5.1 paragraph j (addition)
		(AU-2.5)	The Chief Information Security Officer must review annually, the retention period for audit records and update any USAID defined retention periods, to conform with changes to public laws, directives, regulations, standards, and guidance.	545.3.5.1 paragraph k (addition)
Verify that the agency enforces the controls for access and downloading of personally identifiable information.	AU	Agency regularly reviews audit records, investigates, reports, and takes actions against violations. (AU-6.1)		Is covered by multiple statements already in policy and added for other security control categories. (Reminder Notices)

		(AU-6.6)	Where required by security categorization or system size, the System Owner and System ISSO must employ an automated mechanism to conduct audit monitoring, analysis and reporting.	545.3.5.1 paragraph l (addition)
Verify that Agency policy addresses the protection requirements of personally identifiable information (including that which is accessed remotely or removed from the security perimeter).	IA	Agency develops, disseminates, reviews and updates its identification and authentication policies. (IA-1.1, IA-1.2)		Is covered by multiple statements already in policy and added for other security control categories. (Reminder Notices)
		(IA-1.3)	The System Owner and System ISSO must establish identification and authentication security controls sufficient to meet the security categorization requirements of their information systems, such as UID/password combinations, two-factor authentication (remote token), or biometrics.	545.3.3.1 paragraph h (addition)
		(IA-1.7)	The Chief Information Security Officer must review annually the identification and authentication security controls in use by USAID information systems to determine if they are sufficient to meet the requirements of public laws, directives, regulations, standards, and guidance and require that System Owners and System ISSOs update their security controls if they are determined to be insufficient.	545.3.3.1 paragraph i (addition)

Verify that the Agency is using VPN technologies with two-factor authentication and proper encryption for remote access to systems that contain personally identifiable information.	IA	Agency manages information system authenticators (e.g., tokens, PKI certificates, biometrics, passwords, key cards). (IA-5.1, IA-5.4, IA-5.6)		Is covered by multiple statements already in policy and supporting procedures and added for other security control categories. (Reminder Notices - Passwords, Logical Access Controls, Identification and Authentication, etc.)
		(IA-5.7)	System Owners and System ISSOs must protect identification and authentication mechanisms (such as passwords) from unauthorized disclosure and modification when stored and transmitted, prohibit display when entered, enforce minimum and maximum lifetime restrictions, and prohibit reuse for a specified period.	545.3.3.1 paragraph j (addition)
		(IA-5.8)	Where required by security categorization or system size or complexity, System Owners and Systems ISSOs must use automated identification and authentication mechanism configuration tools.	545.3.3.1 paragraph k (addition)

Verify that Agency policy addresses the protection requirements of personally identifiable information (including that which is accessed remotely or removed from the security perimeter).	MP	Agency develops, disseminates, and periodically reviews and updates its media protection policy and associated controls. (MP-1.1, MP-1.2, MP-1.4)	The definition of media is updated to include all forms of computer readable data that is protected by the Privacy Act, to include reports or other database extracts which require additional security controls.	Is covered by multiple statements already in policy and supporting procedures and added for other security control categories. (Reminder Notice 545.3.2.11)
		(MP-1.2)	The System Owner or System ISSO must report violations of media protection policy to the Chief Information Security Officer and the Chief Privacy Officer.	545.3.2.11 paragraph c (addition)
		(MP-1.2)	Staff must not remove, transport, or store personally identifiable information using any form of electronic media, including government furnished equipment, if the media cannot provide FIPS 140-2 approved encryption, which must be operational if the media is to be transported beyond the USAID security perimeter. The Chief Information Security Officer or System ISSO must authorize all deviations from this policy.	545.3.2.11 paragraph d (addition)
		(MP-1.2)	The System Owner must authorize, in writing, any remote access, transportation or storage of personally identifiable information.	545.3.2.11 paragraph e (addition)
		(MP-1.2)	Staff must provide written justification to the System Owner for any request to remotely access, transport or store personally identifiable information. If authorized by the System Owner, Staff must safeguard the data removed or accessed remotely using security controls approved within the system certification and accreditation.	545.3.2.11 paragraph f (addition)

		(MP-1.7)	The Chief Information Security Officer and Chief Privacy Officer must review annually the media protection policy to determine if it is sufficient to meet the requirements of public laws, directives, regulations, standards, and guidance and require that System Owners and System ISSOs update their security controls if they are determined to be insufficient.	545.3.2.11 paragraph g (addition)
Verify that the Agency is transporting personally identifiable information in encrypted form.	MP	Agency controls information system media (paper and digital) and restricts the pickup, receipt, transfer, and delivery of such media to authorized personnel. (MP-5.1, MP-5.3)		Is covered by multiple statements already in policy and supporting procedures and added for other security control categories. (Reminder Notices)
		(MP-5.5)	The Chief Information Security Officer and Chief Privacy Officer must review annually the media protection policy to determine if it is sufficient to meet the requirements of public laws, directives, regulations, standards, and guidance and require that System Owners and System ISSOs update their security controls if they are determined to be insufficient.	545.3.2.11 paragraph f (addition)
Verify that the Agency is storing personally identifiable informaiton in encrypted form.	PL	Agency establishes and makes available to all users rules of behavior and requires signed acknowledgement from users that they have read and agree to abide by the rules of behavior. (PL-4.1)	For all Missions, general support system networks, and locations with access to AIDNet, System Administrators must use the ADS Chapter 545 Form 545-7 to initiate processing of a user account request.	ADS Chapter 545 (Form ADS 545-7), system-specific RoBs 545.3.1.5 paragraph b (Reminder Notice)
		(PL-4.3)	Examine the rules of behavior to determine if the content is consistent with NIST Special Publication 800-18.	
		(PL-4.6, PL-4.7)		These are requirements to update the user account request process. They will be affected by the implementation of Homeland Security Presidential Directive 12 within this year's annual update cycle.

Verify information categorization of personally identifiable information contained within the Agency's information systems.	PL	Agency conducts privacy impact assessments on its information systems. (PL-5.1, PL-5.2)	The System Owner must conduct a Privacy Impact Assessment (PIA) on each new or existing system to determine the extent, if any, that the system stores, processes or transmits (maintains) personally identifiable information (PII). The System Owner must request approved PIA templates from the Chief Privacy Officer (CPO), privacy@usaid.gov, or download the template from the USAID intranet privacy program web page, http://www.usaid.gov/pp.htm.	545.3.1.8 paragraphs c (addition)
		(PL-5.3)	To comply with FISMA requirements, the System Owner must revalidate their privacy impact assessments annually, and must revalidate their privacy impact assessments when a significant change is made to the information system or the PII data elements collected, shared or transmitted (maintained) by the information system.	545.3.1.8 paragraph d (addition)
		(PL-5.4)	The System Owner may submit questions and comments about the PIA template or procedure, or may request information through the privacy@usaid.gov mail box. The Chief Information Security Officer and Chief Privacy Officer staff must review submitted PIAs and respond to all inquiries made during the consultative/review process.	545.3.1.8 paragraph e (addition)
		(PL-5.4)	The Chief Privacy Officer must annually evaluate the effectiveness of the procedure for conducting privacy impact assessments, and must actively use the evaluation results to improve the procedure.	545.3.1.8 paragraph f (addition)
Verify information categorization of personally identifiable information contained within the Agency's information systems.	RA	Agency categorizes its information systems in accordance with FIPS 199 and documents the results (including supporting rationale) in the System Security Plan. Designated senior-level officials review and approve the security categorizations. (RA-2.1, RA-2.2, RA-2.3)	The Chief Information Security Officer must establish procedures for security categorization that are consistent with FIPS 199 guidelines, using the NIST 800-60, Guide for Mapping Types of Information and Information Systems to Security Categories for USAID System Owners to use when categorizing their information systems.	545.3.1.4 paragraph a (replacement)

		(RA-2.1, RA-2.2, RA-2.3)	During the design phase of their system, the System Owner must conduct a security categorization of the information to be processed by their systems, and include the details of this categorization in the System Security Plan. System Owners cannot categorize systems that process personally identifiable information as "low"--they must be catergorized as at least "moderate."	545.3.1.4 paragraph b (replacement)
		(RA-2.1, RA-2.2, RA-2.3)	The System Owner must submit the security categorization of their USAID systems to the Chief Information Security Officer. System Owners may submit questions and comments about the security categorization procedure to the Chief Information Security Officer at isso@usaid.gov.	545.3.1.4 paragraph h (addition)
		(RA-2.4)	To comply with FISMA requirements, the System Owner must revalidate their system categorization when a significant change is made to the information system or the PII data elements collected, shared or transmitted (maintained) by the information system.	545.3.1.4 paragraph d (addition)
		(RA-2.5)	The Chief Information Security Officer must annually evaluate the effectiveness of the procedure for conducting system categorizations, and must actively use the evaluation results to improve the procedure.	545.3.1.4 paragraph i (addition)
Verify the Agency risk assessment process.	RA	Agency updates its risk assessments annually or whenever there are significant changes to the information system, the facilities where the system resides, or other conditions that may impact the security or accreditation status of the system. (RA-4.1, RA-4.2, RA-4.3, RA-4.4)		545.3.1.4 paragraph c (Reminder Notice)
		(RA-4.5)	The Chief Information Security Officer must annually evaluate the effectiveness of the procedure for conducting risk assessments, and must actively use the evaluation results to improve the procedure.	545.3.1.4 paragraph j (addition)

Verify that Agency policy addresses the protection requirements of personally identifiable information (including that which is accessed remotely or removed from the security perimeter).	SC	Agency develops, disseminates, and periodically reviews/updates its system and communications protection policy. (SC-1.1, SC-1.2, SC-1.4)	The System Owner and System ISSO must implement information system controls consistent with those required based on its security categorization level, to include but not limited to application partitioning, security function isolation, use of FIPS 140-2 cryptographic operations/modules, and protection of internal and external communication between systems and external entities.	These policies and procedures are part of a certification and accreditation, which is required under 545.3.1.7 paragraph a.
		(SC-1.2, SC-1.4)	The System Owner must document the system and communications protection security controls in their System Security Plan.	545.3.1.7 paragraph a procedure (addition)
		(SC-1.7)	The Chief Information Security Officer must annually evaluate the effectiveness of the system and communications protection policies and procedures, and must actively use the evaluation results to improve them.	These policies and procedures are part of a certification and accreditation, which is required under 545.3.1.7 paragraph a.
Verify that the Agency is storing personally identifiable informaiton in encrypted form.	SC	Agency information systems prevent unauthorized and unintended information transfer via shared system resources. (SC-4.1, SC-4.2)	The System Owner and System ISSO must implement information system controls consistent with those required based on its security categorization level, to include but not limited to application partitioning, security function isolation, use of FIPS 140-2 cryptographic operations/modules, and protection of internal and external communication between systems and external entities.	These policies and procedures are part of a certification and accreditation, which is required under 545.3.1.7 paragraph a.
		(SC-4.4)	The Chief Information Security Officer must annually evaluate the effectiveness of the system and communications protection policies and procedures, and must actively use the evaluation results to improve them.	These policies and procedures are part of a certification and accreditation, which is required under 545.3.1.7 paragraph a.

Verify that the Agency is transporting personally identifiable information in encrypted form.	SC	Agency uses only FIPS 140-2 validated cryptographic modules and modes of operation. (SC-13.1)	The System Owner and System ISSO may only use CISO-approved encryption technology within their information systems.	545.3.5.5 (Reminder Notice)