Appendix A: Fiscal Year 2007 Government-wide Summary

Table of Contents

FY 2007 Government-wide Summary -- CIO Reports

Total Number of systems	**10,304**	
Agency systems	**8,951**	
High	1,090	
Moderate	3,273	
Low	4,359	
Not categorized	229	
Contractor systems	**1,353**	
High	121	
Moderate	514	
Low	334	
Not categorized	384	
Certified and Accredited Systems - Total	9,435	**92%**
High	1,156	95%
Moderate	3,486	92%
Low	4,218	90%
Not categorized	575	94%
Tested Security Controls - Total	9,799	95%
High	1,170	97%
Moderate	3,623	96%
Low	4,405	94%
Not categorized	601	98%
Tested Contingency Plans - Total	8,886	86%
High	930	77%
Moderate	3,418	90%
Low	3,981	85%
Not categorized	557	91%
Total # of Systems not Categorized	613	6%
Incidents Reported to USCERT	24,362	
Incidents Reported to Law Enforcement	7,310	
Total Number of Employees	4,140,811	
Employees that received IT security awareness training	3,500,061	85%
Employees that received IT security awareness training using ISSLOB	138,522	
Total Number of Employees with significant IT security responsibilities	98,144	
Employees with significant responsibilities that received training	88,236	90%
Total Costs for providing IT security training	$66,924,255	

The agency explains policies regarding peer-to-peer file sharing in training	Yes	25 agencies
	No	0 agencies
There is an agency-wide security configuration policy	Yes	24 agencies
	No	1 agencies
The agency applies common security configuration established by NIST to application information systems	Rarely (0-50% of the time)	4 agencies
	Sometimes (51-70% of the time)	1 agencies
	Frequently (71-80% of the time)	3 agencies
	Mostly (81-95% of the time)	5 agencies
	Almost Always (96-100% of the time)	12 agencies
The agency has documented in its security policies special procedures for using emerging technologies and countering emerging threats	Yes	24 agencies
	No	1 agencies

-This page left blank intentionally-

FY 2007 Government-wide Summary -- IG Reports

Quality of agency C&A process **1 IG- did not answer (DOD)**	Excellent	4 agencies	
	Good	3 agencies	
	Satisfactory	12 agencies	
	Poor	4 agencies	
	Failing	1 agencies	
The Agency performs oversight and evaluation to ensure information systems used or operated by a contractor of the agency or other organization on behalf of the agency meet the requirements of FISMA, OMB Policy and NIST guidance **1 IG - not applicable (SSA)** **1 IG- did not answer (DOD)**	Rarely (0-50% of the time)		3 agencies
	Sometimes (51-70% of the time)		3 agencies
	Frequently (71-80% of the time)		3 agencies
	Mostly (81-95% of the time)		2 agencies
	Almost Always (96-100% of the time)		12 agencies
The agency has developed an inventory of major information systems, including an identification of interfaces (including those not under control of the agency) **1 IG- did not answer (DOD)**	Approximately 0-50% complete		0 agencies
	Approximately 51-70% complete		1 agencies
	Approximately 71-80% complete		1 agencies
	Approximately 81-95% complete		3 agencies
	Approximately 96-100% complete		19 agencies
The OIG generally agrees with the CIO on the number of agency owned systems	Yes	24 agencies	
	No	1 agencies	
The OIG generally agrees with the CIO on the number of information systems used or operated by a contractor of the agency or other organization on behalf of the agency	Yes	21 agencies	
	No	4 agencies	
The agency inventory is maintained and updated at least annually	Yes	25 agencies	
	No	0 agencies	
The POA&M is an agency wide process, incorporating all known IT Security weaknesses associated with information systems used or operated by the agency or by a contractor of the agency or other organization on behalf of the agency **1 IG - did not answer (DOD)**	Rarely (0-50% of the time)		1 agencies
	Sometimes (51-70% of the time)		4 agencies
	Frequently (71-80% of the time)		5 agencies
	Mostly (81-95% of the time)		1 agencies
	Almost Always (96-100% of the time)		13 agencies
OIG Findings are incorporated into the POA&M process **1 IG - did not answer (DOD)**	Rarely (0-50% of the time)		1 agencies
	Sometimes (51-70% of the time)		1 agencies
	Frequently (71-80% of the time)		1 agencies
	Mostly (81-95% of the time)		6 agencies
	Almost Always (96-100% of the time)		15 agencies
Effective POA&M process? Note: To arrive at "Effective" as reflected in this Appendix, OMB considers a set of IG responses, including how weaknesses are incorporated in the POA&M, how they are prioritized, and how the status of weaknesses is tracked and reported. **1 IG - did not answer (DOD)**	Yes	19 agencies	
	No	5 agencies	
There is an agency wide security configuration policy	Yes	24 agencies	
	No	1 agencies	

FY 2007 Government-wide Summary -- IG Reports (continued)

The agency follows documented policies and procedures for identifying and reporting incidents internally	Yes	19	agencies
1 IG - did not answer (DoD)	No	5	agencies
The agency follows documented policies and procedures for external reporting to law enforcement authorities	Yes	23	agencies
1 IG - did not answer (DoD)	No	1	agencies
The agency follows defined procedures for reporting to the USCERT	Yes	22	agencies
1 IG - did not answer (DoD)	No	2	agencies
The agency has ensured security training and awareness of all employees, including contractors with significant IT security responsibilities	Rarely (0-50% of employees)	0	agencies
1 IG - did not answer (DoD)	Sometimes (51-70% of employees)	1	agencies
	Frequently (71-80% of employees)	5	agencies
	Mostly (81-95% of employees)	8	agencies
	Almost Always (96-100% of employees)	10	agencies
The agency explains policies regarding peer-to-peer file sharing in IT security awareness training, ethics training, or any other agency-wide training	Yes	25	agencies
	No	0	agencies
The agency's PIA process, as discussed in Section D 11.4 (SAOP template), including adherence to existing policy, guidance and standards are	Excellent	4	agencies
2 IG Unaudited (DoC/DoL)	Good	7	agencies
	Satisfactory	8	agencies
	Poor	3	agencies
	Failing	1	agencies
The agency has completed system e-authentication risk assessments	Yes	18	agencies
	No	7	agencies

FY 2007 Government-wide Summary -- Privacy Reports

Systems that contain Federal information in identifiable form	**3,259**	
Agency	2,731	
Contractor	528	
Systems requiring a Privacy Impact Assessment under the E-Gov Act	**1,826**	
Agency	1,584	
Contractor	242	
Systems covered by an existing Privacy Impact Assessment	**1,525**	84%
Agency	1,378	
Contractor	147	
Systems for which a system or records notice (SORN) is required under the Privacy Act	**2,607**	
Agency	2,223	
Contractor	384	
Systems for which a current SORN has been published in the Federal Register	**2,169**	83%
Agency	1,837	
Contractor	332	
The privacy official participates in all agency information privacy compliance activities.	Yes	24 agencies
	No	1 agencies
The privacy official participates in evaluating the ramifications for privacy of legislative, regulatory and other policy proposals, as well as testimony and comments under Circular A-19.	Yes	24 agencies
	No	1 agencies
The privacy official participates in assessing the impact of technology on the privacy of personal information.	Yes	24 agencies
	No	1 agencies
The agency has a training program to ensure all agency personnel and contractors with access to Federal data are generally familiar with information privacy laws, regulations and policies and understand the ramifications of inappropriate access and disclosure?	Yes	25 agencies
	No	0 agencies
The agency has a program for job-specific information privacy training for individuals involved in the administration of personal information or information technology systems, or with significant information security responsibilities.	Yes	21 agencies
	No	4 agencies
The agency has written processes or policies for all listed aspects of Privacy Impact Assessments.	Yes	23 agencies
	No	2 agencies
The agency has written process for determining continued compliance with stated web privacy policies.	Yes	21 agencies
	No	4 agencies
Agency uses persistent tracking technology on any web site.	Yes	6 agencies
	No	19 agencies
Agency annually reviews the use of persistent tracking.	Yes	16 agencies
	No	9 agencies

FY 2007 Government-wide Summary -- Privacy Reports (continued)

Agency has current documentation demonstrating review of compliance with information privacy laws, regulations and policies.	Yes	24 agencies
	No	1 agencies
Agency can provide documentation demonstrating corrective action planned, in progress, or completed to remedy identified compliance deficiencies.	Yes	23 agencies
	No	2 agencies
Agency uses technologies that allow for continuous auditing of compliance with stated privacy policies and practices.	Yes	18 agencies
	No	7 agencies
Agency coordinates with OIG on privacy program oversight	Yes	24 agencies
	No	1 agencies

US Agency for International Development -- CIO Report

Total Number of Systems	26	
Agency Systems	16	
High	0	
Moderate	15	
Low	1	
Not categorized	0	
Contractor Systems	10	
High	0	
Moderate	6	
Low	4	
Not categorized	0	
Certified and Accredited Systems - Total	26	100%
High	0	0%
Moderate	21	100%
Low	5	100%
Not categorized	0	0%
Tested Security Controls - Total	26	100%
High	0	0%
Moderate	21	100%
Low	5	100%
Not categorized	0	0%
Tested Contingency Plans - Total	26	100%
High	0	0%
Moderate	21	100%
Low	5	100%
Not categorized	0	0%
Total # of Systems not Categorized	0	
Incidents Reported to USCERT	185	
Incidents Reported to Law Enforcement	0	
Total Number of Employees	9,065	
Employees that received IT security awareness training	9,065	100%
Employees that received IT security awareness training using ISSLOB	9,065	
Total Number of Employees w/significant IT security responsibilities	206	
Employees with significant responsibilities that received training	195	95%
Total Costs for providing IT security training	$32,352	
The agency explains policies regarding peer-to-peer file sharing in training	Yes	
There is an agency-wide security configuration policy	Yes	
The agency applies common security configuration established by NIST to application information systems	Almost Always (96-100% of the time)	
The agency has documented in its security policies special procedures for using emerging technologies and countering emerging threats	Yes	

US Agency for International Development -- IG Report

Quality of agency C&A process	Excellent
The Agency performs oversight and evaluation to ensure information systems used or operated by a contractor of the agency or other organization on behalf of the agency meet the requirements of FISMA, OMB Policy and NIST guidance	Almost Always (96-100% of the time)
The agency has developed an inventory of major information systems, including an identification of interfaces (including those not under control of the agency)	Approximately 96-100% complete
The OIG generally agrees with the CIO on the number of agency owned systems	Yes
The OIG generally agrees with the CIO on the number of information systems used or operated by a contractor of the agency or other organization on behalf of the agency	Yes
The agency inventory is maintained and updated at least annually	Yes
The POA&M is an agency wide process, incorporating all known IT Security weaknesses associated with information systems used or operated by the agency or by a contractor of the agency or other organization on behalf of the agency	Almost Always (96-100% of the time)
OIG Findings are incorporated into the POA&M process	Almost Always (96-100% of the time)
Effective POA&M process	Yes
There is an agency wide security configuration policy	Yes
The agency follows documented policies and procedures for identifying and reporting incidents internally	Yes
The agency follows documented policies and procedures for external reporting to law enforcement authorities	Yes
The agency follows defined procedures for reporting to the USCERT	Yes
The agency has ensured security training and awareness of all employees, including contractors with significant IT security responsibilities	Almost Always (96-100% of employees)
The agency explains policies regarding peer-to-peer file sharing in IT security awareness training, ethics training, or any other agency-wide training	Yes
Quality of the agency's PIA process, as discussed in Section D 11.4 (SAOP template), including adherence to existing policy, guidance and standards	Good
The agency has completed system e-authentication risk assessments	Yes

US Agency for International Development -- Privacy Report

Systems that contain Federal information in identifiable form	17	
Agency	11	
Contractor	6	
Systems requiring a Privacy Impact Assessment under the E-Gov Act	17	
Agency	11	
Contractor	6	
Systems covered by an existing Privacy Impact Assessment	17	100%
Agency	11	
Contractor	6	
Systems for which a system or records notice (SORN) is required under the Privacy Act	10	
Agency	4	
Contractor	6	
Systems for which a current SORN has been published in the Federal Register	10	100%
Agency	4	
Contractor	6	
The privacy official participates in all agency information privacy compliance activities	Yes	
The privacy official participates in evaluating the ramifications for privacy of legislative, regulatory and other policy proposals, as well as testimony and comments under Circular A-19	Yes	
The privacy official participates in assessing the impact of technology on the privacy of personal information	Yes	
The agency has a training program to ensure all agency personnel and contractors with access to Federal data are generally familiar with information privacy laws, regulations and policies and understand the ramifications of inappropriate access and disclosure	Yes	
The agency has a program for job-specific information privacy training for individuals involved in the administration of personal information or information technology systems, or with significant information security responsibilities	Yes	
The agency has written processes or policies for all listed aspects of Privacy Impact Assessments	Yes	
The agency has written process for determining continued compliance with stated web privacy policies	Yes	
Agency uses persistent tracking technology on any web site	Yes	
Agency annually reviews the use of persistent tracking	Yes	
Agency has current documentation demonstrating review of compliance with information privacy laws, regulations and policies	Yes	
Agency can provide documentation demonstrating corrective action planned, in progress, or completed to remedy identified compliance deficiencies	Yes	
Agency uses technologies that allow for continuous auditing of compliance with stated privacy policies and practices	Yes	
Agency coordinates with OIG on privacy program oversight	Yes	

-This page left blank intentionally-

Department of Agriculture -- CIO Report

Total Number of Systems	242	
Agency Systems	237	
High	25	
Moderate	150	
Low	62	
Not categorized	0	
Contractor Systems	5	
High	0	
Moderate	5	
Low	0	
Not categorized	0	
Certified and Accredited Systems - Total	213	88%
High	24	96%
Moderate	137	88%
Low	52	84%
Not categorized	0	0%
Tested Security Controls - Total	237	98%
High	23	92%
Moderate	153	99%
Low	61	98%
Not categorized	0	0%
Tested Contingency Plans - Total	238	98%
High	25	100%
Moderate	153	99%
Low	60	97%
Not categorized	0	0%
Total # of Systems not Categorized	0	
Incidents Reported to USCERT	368	
Incidents Reported to Law Enforcement	368	
Total Number of Employees	120,076	
Employees that received IT security awareness training	112,852	94%
Employees that received IT security awareness training using ISSLOB	112,852	
Total Number of Employees w/significant IT security responsibilities	1,764	
Employees with significant responsibilities that received training	1,716	97%
Total Costs for providing IT security training	$1,369,224	
The agency explains policies regarding peer-to-peer file sharing in training	Yes	
There is an agency-wide security configuration policy	No	
The agency applies common security configuration established by NIST to application information systems	Rarely (0-50% of the time)	
The agency has documented in its security policies special procedures for using emerging technologies and countering emerging threats	Yes	

Department of Agriculture -- IG Report

Quality of agency C&A process	Poor
The Agency performs oversight and evaluation to ensure information systems used or operated by a contractor of the agency or other organization on behalf of the agency meet the requirements of FISMA, OMB Policy and NIST guidance	Rarely (0-50% of the time)
The agency has developed an inventory of major information systems, including an identification of interfaces (including those not under control of the agency)	The inventory is approximately 71-80% complete
The OIG generally agrees with the CIO on the number of agency owned systems	Yes
The OIG generally agrees with the CIO on the number of information systems used or operated by a contractor of the agency or other organization on behalf of the agency	No
The agency inventory is maintained and updated at least annually	Yes
The POA&M is an agency wide process, incorporating all known IT Security weaknesses associated with information systems used or operated by the agency or by a contractor of the agency or other organization on behalf of the agency	Rarely (0-50% of the time)
OIG Findings are incorporated into the POA&M process	Almost Always (96-100%)
Effective POA&M process	No
There is an agency wide security configuration policy	No
The agency follows documented policies and procedures for identifying and reporting incidents internally	No
The agency follows documented policies and procedures for external reporting to law enforcement authorities	No
The agency follows defined procedures for reporting to the USCERT	No
The agency has ensured security training and awareness of all employees, including contractors with significant IT security responsibilities	Mostly (81-95% of employees)
The agency explains policies regarding peer-to-peer file sharing in IT security awareness training, ethics training, or any other agency-wide training	Yes
Quality of the agency's PIA process, as discussed in Section D 11.4 (SAOP template), including adherence to existing policy, guidance and standards	Poor
The agency has completed system e-authentication risk assessments	No

Department of Agriculture -- Privacy Report

Systems that contain Federal information in identifiable form	101	
Agency	101	
Contractor	0	
Systems requiring a Privacy Impact Assessment under the E-Gov Act	101	
Agency	101	
Contractor	0	
Systems covered by an existing Privacy Impact Assessment	82	81%
Agency	82	
Contractor	0	
Systems for which a system or records notice (SORN) is required under the Privacy Act	101	
Agency	101	
Contractor	0	
Systems for which a current SORN has been published in the Federal Register	51	50%
Agency	51	
Contractor	0	
The privacy official participates in all agency information privacy compliance activities	No	
The privacy official participates in evaluating the ramifications for privacy of legislative, regulatory and other policy proposals, as well as testimony and comments under Circular A-19	No	
The privacy official participates in assessing the impact of technology on the privacy of personal information	No	
The agency has a training program to ensure all agency personnel and contractors with access to Federal data are generally familiar with information privacy laws, regulations and policies and understand the ramifications of inappropriate access and disclosure	Yes	
The agency has a program for job-specific information privacy training for individuals involved in the administration of personal information or information technology systems, or with significant information security responsibilities	No	
The agency has written processes or policies for all listed aspects of Privacy Impact Assessments	No	
The agency has written process for determining continued compliance with stated web privacy policies	Yes	
Agency uses persistent tracking technology on any web site	No	
Agency annually reviews the use of persistent tracking	No	
Agency has current documentation demonstrating review of compliance with information privacy laws, regulations and policies	Yes	
Agency can provide documentation demonstrating corrective action planned, in progress, or completed to remedy identified compliance deficiencies	Yes	
Agency uses technologies that allow for continuous auditing of compliance with stated privacy policies and practices	No	
Agency coordinates with OIG on privacy program oversight	No	

-This page left blank intentionally-

Department of Commerce -- CIO Report

Total Number of Systems	302	
Agency Systems	283	
High	21	
Moderate	198	
Low	53	
Not categorized	11	
Contractor Systems	19	
High	3	
Moderate	14	
Low	2	
Not categorized	0	
Certified and Accredited Systems - Total	291	96%
High	23	96%
Moderate	203	96%
Low	54	98%
Not categorized	11	100%
Tested Security Controls - Total	300	99%
High	24	100%
Moderate	210	99%
Low	55	100%
Not categorized	11	100%
Tested Contingency Plans - Total	288	95%
High	24	100%
Moderate	205	97%
Low	50	91%
Not categorized	9	82%
Total # of Systems not Categorized	11	
Incidents Reported to USCERT	529	
Incidents Reported to Law Enforcement	267	
Total Number of Employees	45,244	
Employees that received IT security awareness training	44,331	98%
Employees that received IT security awareness training using ISSLOB	8,747	
Total Number of Employees w/significant IT security responsibilities	899	
Employees with significant responsibilities that received training	771	86%
Total Costs for providing IT security training	$1,275,411	
The agency explains policies regarding peer-to-peer file sharing in training	Yes	
There is an agency-wide security configuration policy	Yes	
The agency applies common security configuration established by NIST to application information systems	Frequently (71-80% of the time)	
The agency has documented in its security policies special procedures for using emerging technologies and countering emerging threats	Yes	

Department of Commerce -- IG Report

Quality of agency C&A process (includes USPTO)	Poor
The Agency performs oversight and evaluation to ensure information systems used or operated by a contractor of the agency or other organization on behalf of the agency meet the requirements of FISMA, OMB Policy and NIST guidance	Frequently (71-80% of the time)
The agency has developed an inventory of major information systems, including an identification of interfaces (including those not under control of the agency)	The inventory is approximately 96-100% complete
The OIG generally agrees with the CIO on the number of agency owned systems	Yes
The OIG generally agrees with the CIO on the number of information systems used or operated by a contractor of the agency or other organization on behalf of the agency	Yes
The agency inventory is maintained and updated at least annually	Yes
The POA&M is an agency wide process, incorporating all known IT Security weaknesses associated with information systems used or operated by the agency or by a contractor of the agency or other organization on behalf of the agency	Almost Always (96-100% of the time)
OIG Findings are incorporated into the POA&M process	Mostly (81-95% of time)
Effective POA&M process	Yes
There is an agency wide security configuration policy	Yes
The agency follows documented policies and procedures for identifying and reporting incidents internally	Yes
The agency follows documented policies and procedures for external reporting to law enforcement authorities	Yes
The agency follows defined procedures for reporting to the USCERT	Yes
The agency has ensured security training and awareness of all employees, including contractors with significant IT security responsibilities	Almost Always (96-100% of employees)
The agency explains policies regarding peer-to-peer file sharing in IT security awareness training, ethics training, or any other agency-wide training	Yes
Quality of the agency's PIA process, as discussed in Section D 11.4 (SAOP template), including adherence to existing policy, guidance and standards	Unaudited
The agency has completed system e-authentication risk assessments	Yes

Department of Commerce -- Privacy Report

Systems that contain Federal information in identifiable form	42	
Agency	42	
Contractor	0	
Systems requiring a Privacy Impact Assessment under the E-Gov Act	42	
Agency	42	
Contractor	0	
Systems covered by an existing Privacy Impact Assessment	42	100%
Agency	42	
Contractor	0	
Systems for which a system or records notice (SORN) is required under the Privacy Act	41	
Agency	41	
Contractor	0	
Systems for which a current SORN has been published in the Federal Register	41	100%
Agency	41	
Contractor	0	
The privacy official participates in all agency information privacy compliance activities	Yes	
The privacy official participates in evaluating the ramifications for privacy of legislative, regulatory and other policy proposals, as well as testimony and comments under Circular A-19	Yes	
The privacy official participates in assessing the impact of technology on the privacy of personal information	Yes	
The agency has a training program to ensure all agency personnel and contractors with access to Federal data are generally familiar with information privacy laws, regulations and policies and understand the ramifications of inappropriate access and disclosure?	Yes	
The agency has a program for job-specific information privacy training for individuals involved in the administration of personal information or information technology systems, or with significant information security responsibilities	Yes	
The agency has written processes or policies for all listed aspects of Privacy Impact Assessments	Yes	
The agency has written process for determining continued compliance with stated web privacy policies.	Yes	
Agency uses persistent tracking technology on any web site	No	
Agency annually reviews the use of persistent tracking.	Yes	
Agency has current documentation demonstrating review of compliance with information privacy laws, regulations and policies	Yes	
Agency can provide documentation demonstrating corrective action planned, in progress, or completed to remedy identified compliance deficiencies	Yes	
Agency uses technologies that allow for continuous auditing of compliance with stated privacy policies and practices	Yes	
Agency coordinates with OIG on privacy program oversight	Yes	

-This page left blank intentionally-

Department of Defense -- CIO Report

Total Number of Systems	4121	
Agency Systems	4043	
High	277	
Moderate	878	
Low	2888	
Not categorized	0	
Contractor Systems	78	
High	0	
Moderate	20	
Low	58	
Not categorized	0	
Certified and Accredited Systems - Total	3588	87%
High	246	89%
Moderate	806	90%
Low	2536	86%
Not categorized	0	0%
Tested Security Controls - Total	3805	92%
High	258	93%
Moderate	835	93%
Low	2712	92%
Not categorized	0	0%
Tested Contingency Plans - Total	3620	88%
High	260	94%
Moderate	781	87%
Low	2579	88%
Not categorized	0	0%
Total # of Systems not Categorized	0	
Incidents Reported to USCERT	17243	
Incidents Reported to Law Enforcement	5434	
Total Number of Employees	2,497,476	
Employees that received IT security awareness training	1,918,651	77%
Employees that received IT security awareness training using ISSLOB	0	
Total Number of Employees w/significant IT security responsibilities	54,595	
Employees with significant responsibilities that received training	47,901	88%
Total Costs for providing IT security training	$28,962,291	
The agency explains policies regarding peer-to-peer file sharing in training	Yes	
There is an agency-wide security configuration policy	Yes	
The agency applies common security configuration established by NIST to application information systems	Mostly (81-95% of time)	
The agency has documented in its security policies special procedures for using emerging technologies and countering emerging threats	Yes	

Department of Defense -- IG Report

Quality of agency C&A process	Unaudited
The Agency performs oversight and evaluation to ensure information systems used or operated by a contractor of the agency or other organization on behalf of the agency meet the requirements of FISMA, OMB Policy and NIST guidance	Not answered
The agency has developed an inventory of major information systems, including an identification of interfaces (including those not under control of the agency)	Not answered
The OIG generally agrees with the CIO on the number of agency owned systems	No
The OIG generally agrees with the CIO on the number of information systems used or operated by a contractor of the agency or other organization on behalf of the agency	No
The agency inventory is maintained and updated at least annually	Yes
The POA&M is an agency wide process, incorporating all known IT Security weaknesses associated with information systems used or operated by the agency or by a contractor of the agency or other organization on behalf of the agency	Not answered
OIG Findings are incorporated into the POA&M process	Not answered
Effective POA&M process	Not answered
There is an agency wide security configuration policy	Yes
The agency follows documented policies and procedures for identifying and reporting incidents internally	Not answered
The agency follows documented policies and procedures for external reporting to law enforcement authorities	Not answered
The agency follows defined procedures for reporting to the USCERT	Not answered
The agency has ensured security training and awareness of all employees, including contractors with significant IT security responsibilities	Not answered
The agency explains policies regarding peer-to-peer file sharing in IT security awareness training, ethics training, or any other agency-wide training	Yes
Quality of the agency's PIA process, as discussed in Section D 11.4 (SAOP template), including adherence to existing policy, guidance and standards	Failing
The agency has completed system e-authentication risk assessments	Yes

Department of Defense -- Privacy Report

Systems that contain Federal information in identifiable form	648	
Agency	630	
Contractor	18	
Systems requiring a Privacy Impact Assessment under the E-Gov Act	200	
Agency	196	
Contractor	4	
Systems covered by an existing Privacy Impact Assessment	154	77%
Agency	151	
Contractor	3	
Systems for which a system or records notice (SORN) is required under the Privacy Act	564	
Agency	554	
Contractor	10	
Systems for which a current SORN has been published in the Federal Register	287	51%
Agency	283	
Contractor	4	
The privacy official participates in all agency information privacy compliance activities	Yes	
The privacy official participates in evaluating the ramifications for privacy of legislative, regulatory and other policy proposals, as well as testimony and comments under Circular A-19	Yes	
The privacy official participates in assessing the impact of technology on the privacy of personal information	Yes	
The agency has a training program to ensure all agency personnel and contractors with access to Federal data are generally familiar with information privacy laws, regulations and policies and understand the ramifications of inappropriate access and disclosure?	Yes	
The agency has a program for job-specific information privacy training for individuals involved in the administration of personal information or information technology systems, or with significant information security responsibilities	Yes	
The agency has written processes or policies for all listed aspects of Privacy Impact Assessments	Yes	
The agency has written process for determining continued compliance with stated web privacy policies.	Yes	
Agency uses persistent tracking technology on any web site	No	
Agency annually reviews the use of persistent tracking.	No	
Agency has current documentation demonstrating review of compliance with information privacy laws, regulations and policies	Yes	
Agency can provide documentation demonstrating corrective action planned, in progress, or completed to remedy identified compliance deficiencies	Yes	
Agency uses technologies that allow for continuous auditing of compliance with stated privacy policies and practices	No	
Agency coordinates with OIG on privacy program oversight	Yes	

-This page left blank intentionally-

Department of Education -- CIO Report

Total Number of Systems	154	
Agency Systems	85	
High	5	
Moderate	27	
Low	53	
Not categorized	0	
Contractor Systems	69	
High	1	
Moderate	26	
Low	42	
Not categorized	0	
Certified and Accredited Systems - Total	135	88%
High	5	83%
Moderate	50	94%
Low	80	84%
Not categorized	0	0%
Tested Security Controls - Total	140	91%
High	6	100%
Moderate	51	96%
Low	83	87%
Not categorized	0	0%
Tested Contingency Plans - Total	136	88%
High	5	83%
Moderate	50	94%
Low	81	85%
Not categorized	0	0%
Total # of Systems not Categorized	0	
Incidents Reported to USCERT	104	
Incidents Reported to Law Enforcement	97	
Total Number of Employees	12,700	
Employees that received IT security awareness training	11,821	93%
Employees that received IT security awareness training using ISSLOB	0	
Total Number of Employees w/significant IT security responsibilities	1,266	
Employees with significant responsibilities that received training	1,253	99%
Total Costs for providing IT security training	$323,418	
The agency explains policies regarding peer-to-peer file sharing in training	Yes	
There is an agency-wide security configuration policy	Yes	
The agency applies common security configuration established by NIST to application information systems	Sometimes (51-70% of the time)	
The agency has documented in its security policies special procedures for using emerging technologies and countering emerging threats	No	

Department of Education -- IG Report

Quality of agency C&A process	Satisfactory
The Agency performs oversight and evaluation to ensure information systems used or operated by a contractor of the agency or other organization on behalf of the agency meet the requirements of FISMA, OMB Policy and NIST guidance	Almost Always (96-100% of the time)
The agency has developed an inventory of major information systems, including an identification of interfaces (including those not under control of the agency)	Inventory is 96-100% complete
The OIG generally agrees with the CIO on the number of agency owned systems	Yes
The OIG generally agrees with the CIO on the number of information systems used or operated by a contractor of the agency or other organization on behalf of the agency	Yes
The agency inventory is maintained and updated at least annually	Yes
The POA&M is an agency wide process, incorporating all known IT Security weaknesses associated with information systems used or operated by the agency or by a contractor of the agency or other organization on behalf of the agency	Almost Always (96-100% of the time)
OIG Findings are incorporated into the POA&M process	Almost Always (96-100% of the time)
Effective POA&M process	Yes
There is an agency wide security configuration policy	Yes
The agency follows documented policies and procedures for identifying and reporting incidents internally	No
The agency follows documented policies and procedures for external reporting to law enforcement authorities	Yes
The agency follows defined procedures for reporting to the USCERT	Yes
The agency has ensured security training and awareness of all employees, including contractors with significant IT security responsibilities	Mostly (81-95% of employees)
The agency explains policies regarding peer-to-peer file sharing in IT security awareness training, ethics training, or any other agency-wide training	Yes
Quality of the agency's PIA process, as discussed in Section D 11.4 (SAOP template), including adherence to existing policy, guidance and standards	Satisfactory
The agency has completed system e-authentication risk assessments	No

Department of Education -- Privacy Report

Systems that contain Federal information in identifiable form	95	
Agency	54	
Contractor	41	
Systems requiring a Privacy Impact Assessment under the E-Gov Act	21	
Agency	10	
Contractor	11	
Systems covered by an existing Privacy Impact Assessment	20	95%
Agency	9	
Contractor	11	
Systems for which a system or records notice (SORN) is required under the Privacy Act	94	
Agency	51	
Contractor	43	
Systems for which a current SORN has been published in the Federal Register	92	98%
Agency	49	
Contractor	43	
The privacy official participates in all agency information privacy compliance activities	Yes	
The privacy official participates in evaluating the ramifications for privacy of legislative, regulatory and other policy proposals, as well as testimony and comments under Circular A-19	Yes	
The privacy official participates in assessing the impact of technology on the privacy of personal information	Yes	
The agency has a training program to ensure all agency personnel and contractors with access to Federal data are generally familiar with information privacy laws, regulations and policies and understand the ramifications of inappropriate access and disclosure?	Yes	
The agency has a program for job-specific information privacy training for individuals involved in the administration of personal information or information technology systems, or with significant information security responsibilities	No	
The agency has written processes or policies for all listed aspects of Privacy Impact Assessments	Yes	
The agency has written process for determining continued compliance with stated web privacy policies.	Yes	
Agency uses persistent tracking technology on any web site	No	
Agency annually reviews the use of persistent tracking.	No	
Agency has current documentation demonstrating review of compliance with information privacy laws, regulations and policies	Yes	
Agency can provide documentation demonstrating corrective action planned, in progress, or completed to remedy identified compliance deficiencies	No	
Agency uses technologies that allow for continuous auditing of compliance with stated privacy policies and practices	No	
Agency coordinates with OIG on privacy program oversight	Yes	

-This page left blank intentionally-

Department of Energy -- CIO Report

Total Number of Systems	930	
Agency Systems	359	
High	21	
Moderate	104	
Low	35	
Not categorized	199	
Contractor Systems	571	
High	30	
Moderate	122	
Low	43	
Not categorized	376	
Certified and Accredited Systems - Total	904	97%
High	49	96%
Moderate	214	95%
Low	77	99%
Not categorized	564	98%
Tested Security Controls - Total	910	98%
High	49	96%
Moderate	216	96%
Low	73	94%
Not categorized	572	99%
Tested Contingency Plans - Total	842	91%
High	43	84%
Moderate	180	80%
Low	71	91%
Not categorized	548	95%
Total # of Systems not Categorized	575	
Incidents Reported to USCERT	312	
Incidents Reported to Law Enforcement	312	
Total Number of Employees	145,986	
Employees that received IT security awareness training	143,366	98%
Employees that received IT security awareness training using ISSLOB	0	
Total Number of Employees w/significant IT security responsibilities	4,069	
Employees with significant responsibilities that received training	3,433	84%
Total Costs for providing IT security training	$11,002,137	
The agency explains policies regarding peer-to-peer file sharing in training	Yes	
There is an agency-wide security configuration policy	Yes	
The agency applies common security configuration established by NIST to application information systems	Almost Always (96-100% of the time)	
The agency has documented in its security policies special procedures for using emerging technologies and countering emerging threats	Yes	

Department of Energy -- IG Report

Quality of agency C&A process	Satisfactory
The Agency performs oversight and evaluation to ensure information systems used or operated by a contractor of the agency or other organization on behalf of the agency meet the requirements of FISMA, OMB Policy and NIST guidance	Almost Always (96-100% of the time)
The agency has developed an inventory of major information systems, including an identification of interfaces (including those not under control of the agency)	The inventory is approximately 96-100% complete
The OIG generally agrees with the CIO on the number of agency owned systems	Yes
The OIG generally agrees with the CIO on the number of information systems used or operated by a contractor of the agency or other organization on behalf of the agency	Yes
The agency inventory is maintained and updated at least annually	Yes
The POA&M is an agency wide process, incorporating all known IT Security weaknesses associated with information systems used or operated by the agency or by a contractor of the agency or other organization on behalf of the agency	Frequently (71-80% of the time)
OIG Findings are incorporated into the POA&M process	Frequently (71-80% of the time)
Effective POA&M process	Yes
There is an agency wide security configuration policy	Yes
The agency follows documented policies and procedures for identifying and reporting incidents internally	Yes
The agency follows documented policies and procedures for external reporting to law enforcement authorities	Yes
The agency follows defined procedures for reporting to the USCERT	Yes
The agency has ensured security training and awareness of all employees, including contractors with significant IT security responsibilities	Almost Always (96-100% of employees)
The agency explains policies regarding peer-to-peer file sharing in IT security awareness training, ethics training, or any other agency-wide training	Yes
Quality of the agency's PIA process, as discussed in Section D 11.4 (SAOP template), including adherence to existing policy, guidance and standards	Satisfactory
The agency has completed system e-authentication risk assessments	No

Department of Energy -- Privacy Report

Systems that contain Federal information in identifiable form	97	
Agency	66	
Contractor	31	
Systems requiring a Privacy Impact Assessment under the E-Gov Act	50	
Agency	43	
Contractor	7	
Systems covered by an existing Privacy Impact Assessment	21	42%
Agency	21	
Contractor	0	
Systems for which a system or records notice (SORN) is required under the Privacy Act	52	
Agency	48	
Contractor	4	
Systems for which a current SORN has been published in the Federal Register	52	100%
Agency	48	
Contractor	4	
The privacy official participates in all agency information privacy compliance activities	Yes	
The privacy official participates in evaluating the ramifications for privacy of legislative, regulatory and other policy proposals, as well as testimony and comments under Circular A-19	Yes	
The privacy official participates in assessing the impact of technology on the privacy of personal information	Yes	
The agency has a training program to ensure all agency personnel and contractors with access to Federal data are generally familiar with information privacy laws, regulations and policies and understand the ramifications of inappropriate access and disclosure?	Yes	
The agency has a program for job-specific information privacy training for individuals involved in the administration of personal information or information technology systems, or with significant information security responsibilities	Yes	
The agency has written processes or policies for all listed aspects of Privacy Impact Assessments	Yes	
The agency has written process for determining continued compliance with stated web privacy policies	Yes	
Agency uses persistent tracking technology on any web site	No	
Agency annually reviews the use of persistent tracking	No	
Agency has current documentation demonstrating review of compliance with information privacy laws, regulations and policies	Yes	
Agency can provide documentation demonstrating corrective action planned, in progress, or completed to remedy identified compliance deficiencies	Yes	
Agency uses technologies that allow for continuous auditing of compliance with stated privacy policies and practices	Yes	
Agency coordinates with OIG on privacy program oversight	Yes	

-This page left blank intentionally-

Environmental Protection Agency -- CIO Report

Total Number of Systems	171	
Agency Systems	154	
High	1	
Moderate	109	
Low	44	
Not categorized	0	
Contractor Systems	17	
High	0	
Moderate	12	
Low	5	
Not categorized	0	
Certified and Accredited Systems - Total	171	100%
High	1	100%
Moderate	121	100%
Low	49	100%
Not categorized	0	0%
Tested Security Controls - Total	171	100%
High	1	100%
Moderate	121	100%
Low	49	100%
Not categorized	0	0%
Tested Contingency Plans - Total	171	100%
High	1	100%
Moderate	121	100%
Low	49	100%
Not categorized	0	0%
Total # of Systems not Categorized	0	
Incidents Reported to USCERT	141	
Incidents Reported to Law Enforcement	11	
Total Number of Employees	22,259	
Employees that received IT security awareness training	22,259	100%
Employees that received IT security awareness training using ISSLOB	0	
Total Number of Employees w/significant IT security responsibilities	597	
Employees with significant responsibilities that received training	540	90%
Total Costs for providing IT security training	$163,775	
The agency explains policies regarding peer-to-peer file sharing in training	Yes	
There is an agency-wide security configuration policy	Yes	
The agency applies common security configuration established by NIST to application information systems	Almost Always (96-100% of the time)	
The agency has documented in its security policies special procedures for using emerging technologies and countering emerging threats	Yes	

Environmental Protection Agency -- IG Report

Quality of agency C&A process	Satisfactory
The Agency performs oversight and evaluation to ensure information systems used or operated by a contractor of the agency or other organization on behalf of the agency meet the requirements of FISMA, OMB Policy and NIST guidance	Almost Always (96-100% of the time)
The agency has developed an inventory of major information systems, including an identification of interfaces (including those not under control of the agency)	The inventory is approximately 96-100% complete
The OIG generally agrees with the CIO on the number of agency owned systems	Yes
The OIG generally agrees with the CIO on the number of information systems used or operated by a contractor of the agency or other organization on behalf of the agency	Yes
The agency inventory is maintained and updated at least annually	Yes
The POA&M is an agency wide process, incorporating all known IT Security weaknesses associated with information systems used or operated by the agency or by a contractor of the agency or other organization on behalf of the agency	Almost Always (96-100%)
OIG Findings are incorporated into the POA&M process	Almost Always (96-100%)
Effective POA&M process	Yes
There is an agency wide security configuration policy	Yes
The agency follows documented policies and procedures for identifying and reporting incidents internally	Yes
The agency follows documented policies and procedures for external reporting to law enforcement authorities	Yes
The agency follows defined procedures for reporting to the USCERT	Yes
The agency has ensured security training and awareness of all employees, including contractors with significant IT security responsibilities	Almost Always (96-100% of employees)
The agency explains policies regarding peer-to-peer file sharing in IT security awareness training, ethics training, or any other agency-wide training	Yes
Quality of the agency's PIA process, as discussed in Section D 11.4 (SAOP template), including adherence to existing policy, guidance and standards	Satisfactory
The agency has completed system e-authentication risk assessments	No

Environmental Protection Agency -- Privacy Report

Systems that contain Federal information in identifiable form	36	
Agency	34	
Contractor	2	
Systems requiring a Privacy Impact Assessment under the E-Gov Act	36	
Agency	34	
Contractor	2	
Systems covered by an existing Privacy Impact Assessment	36	100%
Agency	34	
Contractor	2	
Systems for which a system or records notice (SORN) is required under the Privacy Act	31	
Agency	29	
Contractor	2	
Systems for which a current SORN has been published in the Federal Register	31	100%
Agency	29	
Contractor	2	
The privacy official participates in all agency information privacy compliance activities	Yes	
The privacy official participates in evaluating the ramifications for privacy of legislative, regulatory and other policy proposals, as well as testimony and comments under Circular A-19	Yes	
The privacy official participates in assessing the impact of technology on the privacy of personal information	Yes	
The agency has a training program to ensure all agency personnel and contractors with access to Federal data are generally familiar with information privacy laws, regulations and policies and understand the ramifications of inappropriate access and disclosure?	Yes	
The agency has a program for job-specific information privacy training for individuals involved in the administration of personal information or information technology systems, or with significant information security responsibilities	No	
The agency has written processes or policies for all listed aspects of Privacy Impact Assessments	Yes	
The agency has written process for determining continued compliance with stated web privacy policies	No	
Agency uses persistent tracking technology on any web site	No	
Agency annually reviews the use of persistent tracking	No	
Agency has current documentation demonstrating review of compliance with information privacy laws, regulations and policies	No	
Agency can provide documentation demonstrating corrective action planned, in progress, or completed to remedy identified compliance deficiencies	No	
Agency uses technologies that allow for continuous auditing of compliance with stated privacy policies and practices	No	
Agency coordinates with OIG on privacy program oversight	Yes	

-This page left blank intentionally-

General Services Administration -- CIO Report

Total Number of Systems	78	
Agency Systems	40	
High	0	
Moderate	31	
Low	9	
Not categorized	0	
Contractor Systems	38	
High	1	
Moderate	26	
Low	11	
Not categorized	0	
Certified and Accredited Systems - Total	78	100%
High	1	100%
Moderate	57	100%
Low	20	100%
Not categorized	0	0%
Tested Security Controls - Total	78	100%
High	1	100%
Moderate	57	100%
Low	20	100%
Not categorized	0	0%
Tested Contingency Plans - Total	78	100%
High	1	100%
Moderate	57	100%
Low	20	100%
Not categorized	0	0%
Total # of Systems not Categorized	0	
Incidents Reported to USCERT	65	
Incidents Reported to Law Enforcement	29	
Total Number of Employees	14,806	
Employees that received IT security awareness training	14,806	100%
Employees that received IT security awareness training using ISSLOB	0	
Total Number of Employees w/significant IT security responsibilities	1,023	
Employees with significant responsibilities that received training	1,023	100%
Total Costs for providing IT security training	$150,000	
The agency explains policies regarding peer-to-peer file sharing in training	Yes	
There is an agency-wide security configuration policy	Yes	
The agency applies common security configuration established by NIST to application information systems	Mostly (81-95% of the time)	
The agency has documented in its security policies special procedures for using emerging technologies and countering emerging threats	Yes	

General Services Administration -- IG Report

Quality of agency C&A process	Satisfactory
The Agency performs oversight and evaluation to ensure information systems used or operated by a contractor of the agency or other organization on behalf of the agency meet the requirements of FISMA, OMB Policy and NIST guidance	Sometimes (51-70% of the time)
The agency has developed an inventory of major information systems, including an identification of interfaces (including those not under control of the agency)	The inventory is approximately 96-100% complete
The OIG generally agrees with the CIO on the number of agency owned systems	Yes
The OIG generally agrees with the CIO on the number of information systems used or operated by a contractor of the agency or other organization on behalf of the agency	Yes
The agency inventory is maintained and updated at least annually	Yes
The POA&M is an agency wide process, incorporating all known IT Security weaknesses associated with information systems used or operated by the agency or by a contractor of the agency or other organization on behalf of the agency	Almost Always (96-100%)
OIG Findings are incorporated into the POA&M process	Almost Always (96-100%)
Effective POA&M process	Yes
There is an agency wide security configuration policy	Yes
The agency follows documented policies and procedures for identifying and reporting incidents internally	Yes
The agency follows documented policies and procedures for external reporting to law enforcement authorities	Yes
The agency follows defined procedures for reporting to the USCERT	Yes
The agency has ensured security training and awareness of all employees, including contractors with significant IT security responsibilities	Almost Always (96-100% of employees)
The agency explains policies regarding peer-to-peer file sharing in IT security awareness training, ethics training, or any other agency-wide training	Yes
Quality of the agency's PIA process, as discussed in Section D 11.4 (SAOP template), including adherence to existing policy, guidance and standards	Satisfactory
The agency has completed system e-authentication risk assessments	Yes

General Services Administration -- Privacy Report

Systems that contain Federal information in identifiable form	40	
Agency	28	
Contractor	12	
Systems requiring a Privacy Impact Assessment under the E-Gov Act	16	
Agency	8	
Contractor	8	
Systems covered by an existing Privacy Impact Assessment	16	100%
Agency	8	
Contractor	8	
Systems for which a system or records notice (SORN) is required under the Privacy Act	40	
Agency	28	
Contractor	12	
Systems for which a current SORN has been published in the Federal Register	40	100%
Agency	28	
Contractor	12	
The privacy official participates in all agency information privacy compliance activities	Yes	
The privacy official participates in evaluating the ramifications for privacy of legislative, regulatory and other policy proposals, as well as testimony and comments under Circular A-19	Yes	
The privacy official participates in assessing the impact of technology on the privacy of personal information	Yes	
The agency has a training program to ensure all agency personnel and contractors with access to Federal data are generally familiar with information privacy laws, regulations and policies and understand the ramifications of inappropriate access and disclosure?	Yes	
The agency has a program for job-specific information privacy training for individuals involved in the administration of personal information or information technology systems, or with significant information security responsibilities	No	
The agency has written processes or policies for all listed aspects of Privacy Impact Assessments	Yes	
The agency has written process for determining continued compliance with stated web privacy policies	Yes	
Agency uses persistent tracking technology on any web site	No	
Agency annually reviews the use of persistent tracking	Yes	
Agency has current documentation demonstrating review of compliance with information privacy laws, regulations and policies	Yes	
Agency can provide documentation demonstrating corrective action planned, in progress, or completed to remedy identified compliance deficiencies	Yes	
Agency uses technologies that allow for continuous auditing of compliance with stated privacy policies and practices	Yes	
Agency coordinates with OIG on privacy program oversight	Yes	

-This page left blank intentionally-

Department of Health and Human Services -- CIO Report

Total Number of Systems	148	
Agency Systems	126	
High	40	
Moderate	71	
Low	15	
Not categorized	0	
Contractor Systems	22	
High	7	
Moderate	11	
Low	4	
Not categorized	0	
Certified and Accredited Systems - Total	148	100%
High	47	100%
Moderate	82	100%
Low	19	100%
Not categorized	0	0%
Tested Security Controls - Total	148	100%
High	47	100%
Moderate	82	100%
Low	19	100%
Not categorized	0	0%
Tested Contingency Plans - Total	148	100%
High	47	100%
Moderate	82	100%
Low	19	100%
Not categorized	0	0%
Total # of Systems not Categorized	0	
Incidents Reported to USCERT	40	
Incidents Reported to Law Enforcement	8	
Total Number of Employees	87,213	
Employees that received IT security awareness training	86,540	99%
Employees that received IT security awareness training using ISSLOB	0	
Total Number of Employees w/significant IT security responsibilities	2,517	
Employees with significant responsibilities that received training	2,444	97%
Total Costs for providing IT security training	$2,491,418	
The agency explains policies regarding peer-to-peer file sharing in training	Yes	
There is an agency-wide security configuration policy	Yes	
The agency applies common security configuration established by NIST to application information systems	Almost Always (96-100% of the time)	
The agency has documented in its security policies special procedures for using emerging technologies and countering emerging threats	Yes	

Department of Health and Human Services -- IG Report

Quality of agency C&A process	Good
The Agency performs oversight and evaluation to ensure information systems used or operated by a contractor of the agency or other organization on behalf of the agency meet the requirements of FISMA, OMB Policy and NIST guidance	Mostly (81-95% of the time)
The agency has developed an inventory of major information systems, including an identification of interfaces (including those not under control of the agency)	Inventory is 96-100% complete
The OIG generally agrees with the CIO on the number of agency owned systems	Yes
The OIG generally agrees with the CIO on the number of information systems used or operated by a contractor of the agency or other organization on behalf of the agency	Yes
The agency inventory is maintained and updated at least annually	Yes
The POA&M is an agency wide process, incorporating all known IT Security weaknesses associated with information systems used or operated by the agency or by a contractor of the agency or other organization on behalf of the agency	Frequently (71-80% of the time)
OIG Findings are incorporated into the POA&M process	Mostly (81-95% of the time)
Effective POA&M process	Yes
There is an agency wide security configuration policy	Yes
The agency follows documented policies and procedures for identifying and reporting incidents internally	Yes
The agency follows documented policies and procedures for external reporting to law enforcement authorities	Yes
The agency follows defined procedures for reporting to the USCERT	Yes
The agency has ensured security training and awareness of all employees, including contractors with significant IT security responsibilities	Mostly (81-95% of the time)
The agency explains policies regarding peer-to-peer file sharing in IT security awareness training, ethics training, or any other agency-wide training	Yes
Quality of the agency's PIA process, as discussed in Section D 11.4 (SAOP template), including adherence to existing policy, guidance and standards	Excellent
The agency has completed system e-authentication risk assessments	Yes

Department of Health and Human Services -- Privacy Report

Systems that contain Federal information in identifiable form	87	
Agency	79	
Contractor	8	
Systems requiring a Privacy Impact Assessment under the E-Gov Act	87	
Agency	79	
Contractor	8	
Systems covered by an existing Privacy Impact Assessment	87	100%
Agency	79	
Contractor	8	
Systems for which a system or records notice (SORN) is required under the Privacy Act	63	
Agency	59	
Contractor	4	
Systems for which a current SORN has been published in the Federal Register	62	98%
Agency	58	
Contractor	4	
The privacy official participates in all agency information privacy compliance activities	Yes	
The privacy official participates in evaluating the ramifications for privacy of legislative, regulatory and other policy proposals, as well as testimony and comments under Circular A-19	Yes	
The privacy official participates in assessing the impact of technology on the privacy of personal information	Yes	
The agency has a training program to ensure all agency personnel and contractors with access to Federal data are generally familiar with information privacy laws, regulations and policies and understand the ramifications of inappropriate access and disclosure?	Yes	
The agency has a program for job-specific information privacy training for individuals involved in the administration of personal information or information technology systems, or with significant information security responsibilities	Yes	
The agency has written processes or policies for all listed aspects of Privacy Impact Assessments	Yes	
The agency has written process for determining continued compliance with stated web privacy policies	Yes	
Agency uses persistent tracking technology on any web site	Yes	
Agency annually reviews the use of persistent tracking	Yes	
Agency has current documentation demonstrating review of compliance with information privacy laws, regulations and policies	Yes	
Agency can provide documentation demonstrating corrective action planned, in progress, or completed to remedy identified compliance deficiencies	Yes	
Agency uses technologies that allow for continuous auditing of compliance with stated privacy policies and practices	Yes	
Agency coordinates with OIG on privacy program oversight	Yes	

-This page left blank intentionally-

Department of Homeland Security -- CIO Report

Total Number of Systems	603	
Agency Systems	396	
High	136	
Moderate	210	
Low	49	
Not categorized	1	
Contractor Systems	207	
High	58	
Moderate	118	
Low	31	
Not categorized	0	
Certified and Accredited Systems - Total	506	84%
High	182	94%
Moderate	251	77%
Low	73	91%
Not categorized	0	0%
Tested Security Controls - Total	579	96%
High	186	96%
Moderate	325	99%
Low	68	85%
Not categorized	0	0%
Tested Contingency Plans - Total	507	84%
High	174	90%
Moderate	302	92%
Low	31	39%
Not categorized	0	0%
Total # of Systems not Categorized	1	
Incidents Reported to USCERT	636	
Incidents Reported to Law Enforcement	61	
Total Number of Employees	220,149	
Employees that received IT security awareness training	209,309	95%
Employees that received IT security awareness training using ISSLOB	0	
Total Number of Employees w/significant IT security responsibilities	1,372	
Employees with significant responsibilities that received training	1,352	99%
Total Costs for providing IT security training	$3,109,606	
The agency explains policies regarding peer-to-peer file sharing in training	Yes	
There is an agency-wide security configuration policy	Yes	
The agency applies common security configuration established by NIST to application information systems	Almost Always (96-100% of the time)	
The agency has documented in its security policies special procedures for using emerging technologies and countering emerging threats	Yes	

Department of Homeland Security -- IG Report

Quality of agency C&A process	Satisfactory
The Agency performs oversight and evaluation to ensure information systems used or operated by a contractor of the agency or other organization on behalf of the agency meet the requirements of FISMA, OMB Policy and NIST guidance	Almost Always (96-100% of the time)
The agency has developed an inventory of major information systems, including an identification of interfaces (including those not under control of the agency)	The inventory is approximately 96-100% complete
The OIG generally agrees with the CIO on the number of agency owned systems	Yes
The OIG generally agrees with the CIO on the number of information systems used or operated by a contractor of the agency or other organization on behalf of the agency	Yes
The agency inventory is maintained and updated at least annually	Yes
The POA&M is an agency wide process, incorporating all known IT Security weaknesses associated with information systems used or operated by the agency or by a contractor of the agency or other organization on behalf of the agency	Almost Always (96-100% of the time)
OIG Findings are incorporated into the POA&M process	Mostly (81-95% of the time)
Effective POA&M process	Yes
There is an agency wide security configuration policy	Yes
The agency follows documented policies and procedures for identifying and reporting incidents internally	Yes
The agency follows documented policies and procedures for external reporting to law enforcement authorities	Yes
The agency follows defined procedures for reporting to the USCERT	Yes
The agency has ensured security training and awareness of all employees, including contractors with significant IT security responsibilities	Mostly (81-95% of employees)
The agency explains policies regarding peer-to-peer file sharing in IT security awareness training, ethics training, or any other agency-wide training	Yes
Quality of the agency's PIA process, as discussed in Section D 11.4 (SAOP template), including adherence to existing policy, guidance and standards	Good
The agency has completed system e-authentication risk assessments	Yes

Department of Homeland Security -- Privacy Report

Systems that contain Federal information in identifiable form	254	
Agency	127	
Contractor	127	
Systems requiring a Privacy Impact Assessment under the E-Gov Act	163	
Agency	76	
Contractor	87	
Systems covered by an existing Privacy Impact Assessment	42	26%
Agency	21	
Contractor	21	
Systems for which a system or records notice (SORN) is required under the Privacy Act	224	
Agency	113	
Contractor	111	
Systems for which a current SORN has been published in the Federal Register	148	66%
Agency	79	
Contractor	69	
The privacy official participates in all agency information privacy compliance activities	Yes	
The privacy official participates in evaluating the ramifications for privacy of legislative, regulatory and other policy proposals, as well as testimony and comments under Circular A-19	Yes	
The privacy official participates in assessing the impact of technology on the privacy of personal information	Yes	
The agency has a training program to ensure all agency personnel and contractors with access to Federal data are generally familiar with information privacy laws, regulations and policies and understand the ramifications of inappropriate access and disclosure?	Yes	
The agency has a program for job-specific information privacy training for individuals involved in the administration of personal information or information technology systems, or with significant information security responsibilities	Yes	
The agency has written processes or policies for all listed aspects of Privacy Impact Assessments	Yes	
The agency has written process for determining continued compliance with stated web privacy policies	No	
Agency uses persistent tracking technology on any web site	No	
Agency annually reviews the use of persistent tracking	Yes	
Agency has current documentation demonstrating review of compliance with information privacy laws, regulations and policies	Yes	
Agency can provide documentation demonstrating corrective action planned, in progress, or completed to remedy identified compliance deficiencies	Yes	
Agency uses technologies that allow for continuous auditing of compliance with stated privacy policies and practices	No	
Agency coordinates with OIG on privacy program oversight	Yes	

-This page left blank intentionally-

Department of Housing and Urban Development -- CIO Report

Total Number of Systems	101	
Agency Systems	85	
High	5	
Moderate	63	
Low	17	
Not categorized	0	
Contractor Systems	16	
High	0	
Moderate	14	
Low	2	
Not categorized	0	
Certified and Accredited Systems - Total	101	100%
High	5	100%
Moderate	77	100%
Low	19	100%
Not categorized	0	0%
Tested Security Controls - Total	101	100%
High	5	100%
Moderate	77	100%
Low	19	100%
Not categorized	0	0%
Tested Contingency Plans - Total	82	81%
High	5	100%
Moderate	77	100%
Low	0	0%
Not categorized	0	0%
Total # of Systems not Categorized	0	
Incidents Reported to USCERT	26	
Incidents Reported to Law Enforcement	2	
Total Number of Employees	9,130	
Employees that received IT security awareness training	8,872	97%
Employees that received IT security awareness training using ISSLOB	0	
Total Number of Employees w/significant IT security responsibilities	312	
Employees with significant responsibilities that received training	302	97%
Total Costs for providing IT security training	$98,000	
The agency explains policies regarding peer-to-peer file sharing in training	Yes	
There is an agency-wide security configuration policy	Yes	
The agency applies common security configuration established by NIST to application information systems	Almost Always (96-100% of the time)	
The agency has documented in its security policies special procedures for using emerging technologies and countering emerging threats	Yes	

Department of Housing and Urban Development -- IG Report

Quality of agency C&A process	Satisfactory
The Agency performs oversight and evaluation to ensure information systems used or operated by a contractor of the agency or other organization on behalf of the agency meet the requirements of FISMA, OMB Policy and NIST guidance	Almost Always(96-100% of the time)
The agency has developed an inventory of major information systems, including an identification of interfaces (including those not under control of the agency)	The inventory is approximately 96-100% complete
The OIG generally agrees with the CIO on the number of agency owned systems	Yes
The OIG generally agrees with the CIO on the number of information systems used or operated by a contractor of the agency or other organization on behalf of the agency	Yes
The agency inventory is maintained and updated at least annually	Yes
The POA&M is an agency wide process, incorporating all known IT Security weaknesses associated with information systems used or operated by the agency or by a contractor of the agency or other organization on behalf of the agency	Almost Always (96-100%)
OIG Findings are incorporated into the POA&M process	Almost Always (96-100%)
Effective POA&M process	Yes
There is an agency wide security configuration policy	Yes
The agency follows documented policies and procedures for identifying and reporting incidents internally	Yes
The agency follows documented policies and procedures for external reporting to law enforcement authorities	Yes
The agency follows defined procedures for reporting to the USCERT	No
The agency has ensured security training and awareness of all employees, including contractors with significant IT security responsibilities	Almost Always (96-100% of employees)
The agency explains policies regarding peer-to-peer file sharing in IT security awareness training, ethics training, or any other agency-wide training	Yes
Quality of the agency's PIA process, as discussed in Section D 11.4 (SAOP template), including adherence to existing policy, guidance and standards	Good
The agency has completed system e-authentication risk assessments	No

Department of Housing and Urban Development -- Privacy Report

Systems that contain Federal information in identifiable form	72	
Agency	72	
Contractor	0	
Systems requiring a Privacy Impact Assessment under the E-Gov Act	19	
Agency	19	
Contractor	0	
Systems covered by an existing Privacy Impact Assessment	19	100%
Agency	19	
Contractor	0	
Systems for which a system or records notice (SORN) is required under the Privacy Act	42	
Agency	42	
Contractor	0	
Systems for which a current SORN has been published in the Federal Register	42	100%
Agency	42	
Contractor	0	
The privacy official participates in all agency information privacy compliance activities	Yes	
The privacy official participates in evaluating the ramifications for privacy of legislative, regulatory and other policy proposals, as well as testimony and comments under Circular A-19	Yes	
The privacy official participates in assessing the impact of technology on the privacy of personal information	Yes	
The agency has a training program to ensure all agency personnel and contractors with access to Federal data are generally familiar with information privacy laws, regulations and policies and understand the ramifications of inappropriate access and disclosure?	Yes	
The agency has a program for job-specific information privacy training for individuals involved in the administration of personal information or information technology systems, or with significant information security responsibilities	Yes	
The agency has written processes or policies for all listed aspects of Privacy Impact Assessments	Yes	
The agency has written process for determining continued compliance with stated web privacy policies	Yes	
Agency uses persistent tracking technology on any web site	No	
Agency annually reviews the use of persistent tracking	No	
Agency has current documentation demonstrating review of compliance with information privacy laws, regulations and policies	Yes	
Agency can provide documentation demonstrating corrective action planned, in progress, or completed to remedy identified compliance deficiencies	Yes	
Agency uses technologies that allow for continuous auditing of compliance with stated privacy policies and practices	No	
Agency coordinates with OIG on privacy program oversight	Yes	

-This page left blank intentionally-

Department of Interior -- CIO Report

Total Number of Systems	151	
Agency Systems	133	
High	5	
Moderate	102	
Low	26	
Not categorized	0	
Contractor Systems	18	
High	1	
Moderate	11	
Low	6	
Not categorized	0	
Certified and Accredited Systems - Total	145	96%
High	6	100%
Moderate	107	95%
Low	32	100%
Not categorized	0	0%
Tested Security Controls - Total	145	96%
High	6	100%
Moderate	108	96%
Low	31	97%
Not categorized	0	0%
Tested Contingency Plans - Total	122	81%
High	5	83%
Moderate	92	81%
Low	25	78%
Not categorized	0	0%
Total # of Systems not Categorized	0	
Incidents Reported to USCERT	166	
Incidents Reported to Law Enforcement	77	
Total Number of Employees	83,197	
Employees that received IT security awareness training	83,197	100%
Employees that received IT security awareness training using ISSLOB	0	
Total Number of Employees w/significant IT security responsibilities	2,962	
Employees with significant responsibilities that received training	2,410	81%
Total Costs for providing IT security training	$225,002	
The agency explains policies regarding peer-to-peer file sharing in training	Yes	
There is an agency-wide security configuration policy	Yes	
The agency applies common security configuration established by NIST to application information systems	Frequently (71-80% of the time)	
The agency has documented in its security policies special procedures for using emerging technologies and countering emerging threats	Yes	

Department of Interior -- IG Report

Quality of agency C&A process	Poor
The Agency performs oversight and evaluation to ensure information systems used or operated by a contractor of the agency or other organization on behalf of the agency meet the requirements of FISMA, OMB Policy and NIST guidance	Frequently (71-80% of the time)
The agency has developed an inventory of major information systems, including an identification of interfaces (including those not under control of the agency)	The inventory is approximately 96-100% complete
The OIG generally agrees with the CIO on the number of agency owned systems	Yes
The OIG generally agrees with the CIO on the number of information systems used or operated by a contractor of the agency or other organization on behalf of the agency	Yes
The agency inventory is maintained and updated at least annually	Yes
The POA&M is an agency wide process, incorporating all known IT Security weaknesses associated with information systems used or operated by the agency or by a contractor of the agency or other organization on behalf of the agency	Frequently (71-80% of the time)
OIG Findings are incorporated into the POA&M process	Mostly (81-95% of the time)
Effective POA&M process	No
There is an agency wide security configuration policy	Yes
The agency follows documented policies and procedures for identifying and reporting incidents internally	Yes
The agency follows documented policies and procedures for external reporting to law enforcement authorities	Yes
The agency follows defined procedures for reporting to the USCERT	Yes
The agency has ensured security training and awareness of all employees, including contractors with significant IT security responsibilities	Mostly (81-95% of employees)
The agency explains policies regarding peer-to-peer file sharing in IT security awareness training, ethics training, or any other agency-wide training	Yes
Quality of the agency's PIA process, as discussed in Section D 11.4 (SAOP template), including adherence to existing policy, guidance and standards	Poor
The agency has completed system e-authentication risk assessments	Yes

Department of Interior -- Privacy Report

Systems that contain Federal information in identifiable form	134	
Agency	128	
Contractor	6	
Systems requiring a Privacy Impact Assessment under the E-Gov Act	76	
Agency	72	
Contractor	4	
Systems covered by an existing Privacy Impact Assessment	76	100%
Agency	72	
Contractor	4	
Systems for which a system or records notice (SORN) is required under the Privacy Act	64	
Agency	60	
Contractor	4	
Systems for which a current SORN has been published in the Federal Register	64	100%
Agency	60	
Contractor	4	
The privacy official participates in all agency information privacy compliance activities	Yes	
The privacy official participates in evaluating the ramifications for privacy of legislative, regulatory and other policy proposals, as well as testimony and comments under Circular A-19	Yes	
The privacy official participates in assessing the impact of technology on the privacy of personal information	Yes	
The agency has a training program to ensure all agency personnel and contractors with access to Federal data are generally familiar with information privacy laws, regulations and policies and understand the ramifications of inappropriate access and disclosure?	Yes	
The agency has a program for job-specific information privacy training for individuals involved in the administration of personal information or information technology systems, or with significant information security responsibilities	Yes	
The agency has written processes or policies for all listed aspects of Privacy Impact Assessments	Yes	
The agency has written process for determining continued compliance with stated web privacy policies	Yes	
Agency uses persistent tracking technology on any web site	Yes	
Agency annually reviews the use of persistent tracking	Yes	
Agency has current documentation demonstrating review of compliance with information privacy laws, regulations and policies	Yes	
Agency can provide documentation demonstrating corrective action planned, in progress, or completed to remedy identified compliance deficiencies	Yes	
Agency uses technologies that allow for continuous auditing of compliance with stated privacy policies and practices	Yes	
Agency coordinates with OIG on privacy program oversight	Yes	

-This page left blank intentionally-

Department of Justice -- CIO Report

Total Number of Systems	225	
Agency Systems	215	
High	78	
Moderate	90	
Low	47	
Not categorized	0	
Contractor Systems	10	
High	3	
Moderate	4	
Low	3	
Not categorized	0	
Certified and Accredited Systems - Total	225	100%
High	81	100%
Moderate	94	100%
Low	50	100%
Not categorized	0	0%
Tested Security Controls - Total	225	100%
High	81	100%
Moderate	94	100%
Low	50	100%
Not categorized	0	0%
Tested Contingency Plans - Total	225	100%
High	81	100%
Moderate	94	100%
Low	50	100%
Not categorized	0	0%
Total # of Systems not Categorized	0	
Incidents Reported to USCERT	802	
Incidents Reported to Law Enforcement	133	
Total Number of Employees	125,424	
Employees that received IT security awareness training	121,704	97%
Employees that received IT security awareness training using ISSLOB	0	
Total Number of Employees w/significant IT security responsibilities	1,212	
Employees with significant responsibilities that received training	1,179	97%
Total Costs for providing IT security training	$2,982,477	
The agency explains policies regarding peer-to-peer file sharing in training	Yes	
There is an agency-wide security configuration policy	Yes	
The agency applies common security configuration established by NIST to application information systems	Almost Always (96-100% of the time)	
The agency has documented in its security policies special procedures for using emerging technologies and countering emerging threats	Yes	

Department of Justice -- IG Report

Quality of agency C&A process	Excellent
The Agency performs oversight and evaluation to ensure information systems used or operated by a contractor of the agency or other organization on behalf of the agency meet the requirements of FISMA, OMB Policy and NIST guidance	Almost Always (96-100% of the time)
The agency has developed an inventory of major information systems, including an identification of interfaces (including those not under control of the agency)	The inventory is approximately 96-100% complete
The OIG generally agrees with the CIO on the number of agency owned systems	Yes
The OIG generally agrees with the CIO on the number of information systems used or operated by a contractor of the agency or other organization on behalf of the agency	Yes
The agency inventory is maintained and updated at least annually	Yes
The POA&M is an agency wide process, incorporating all known IT Security weaknesses associated with information systems used or operated by the agency or by a contractor of the agency or other organization on behalf of the agency	Almost Always (96-100% of the time)
OIG Findings are incorporated into the POA&M process	Almost Always (96-100% of the time)
Effective POA&M process	Yes
There is an agency wide security configuration policy	Yes
The agency follows documented policies and procedures for identifying and reporting incidents internally	Yes
The agency follows documented policies and procedures for external reporting to law enforcement authorities	Yes
The agency follows defined procedures for reporting to the USCERT	Yes
The agency has ensured security training and awareness of all employees, including contractors with significant IT security responsibilities	Almost Always (96-100% of employees)
The agency explains policies regarding peer-to-peer file sharing in IT security awareness training, ethics training, or any other agency-wide training	Yes
Quality of the agency's PIA process, as discussed in Section D 11.4 (SAOP template), including adherence to existing policy, guidance and standards	Excellent
The agency has completed system e-authentication risk assessments	Yes

Department of Justice -- Privacy Report

Systems that contain Federal information in identifiable form	173	
Agency	164	
Contractor	9	
Systems requiring a Privacy Impact Assessment under the E-Gov Act	58	
Agency	53	
Contractor	5	
Systems covered by an existing Privacy Impact Assessment	54	93%
Agency	49	
Contractor	5	
Systems for which a system or records notice (SORN) is required under the Privacy Act	140	
Agency	132	
Contractor	8	
Systems for which a current SORN has been published in the Federal Register	140	100%
Agency	132	
Contractor	8	
The privacy official participates in all agency information privacy compliance activities	Yes	
The privacy official participates in evaluating the ramifications for privacy of legislative, regulatory and other policy proposals, as well as testimony and comments under Circular A-19	Yes	
The privacy official participates in assessing the impact of technology on the privacy of personal information	Yes	
The agency has a training program to ensure all agency personnel and contractors with access to Federal data are generally familiar with information privacy laws, regulations and policies and understand the ramifications of inappropriate access and disclosure?	Yes	
The agency has a program for job-specific information privacy training for individuals involved in the administration of personal information or information technology systems, or with significant information security responsibilities	Yes	
The agency has written processes or policies for all listed aspects of Privacy Impact Assessments	Yes	
The agency has written process for determining continued compliance with stated web privacy policies	Yes	
Agency uses persistent tracking technology on any web site	No	
Agency annually reviews the use of persistent tracking	Yes	
Agency has current documentation demonstrating review of compliance with information privacy laws, regulations and policies	Yes	
Agency can provide documentation demonstrating corrective action planned, in progress, or completed to remedy identified compliance deficiencies	Yes	
Agency uses technologies that allow for continuous auditing of compliance with stated privacy policies and practices	Yes	
Agency coordinates with OIG on privacy program oversight	Yes	

-This page left blank intentionally-

Department of Labor -- CIO Report

Total Number of Systems	71	
Agency Systems	60	
High	1	
Moderate	59	
Low	0	
Not categorized	0	
Contractor Systems	11	
High	1	
Moderate	10	
Low	0	
Not categorized	0	
Certified and Accredited Systems - Total	71	100%
High	2	100%
Moderate	69	100%
Low	0	0%
Not categorized	0	0%
Tested Security Controls - Total	71	100%
High	2	100%
Moderate	69	100%
Low	0	0%
Not categorized	0	0%
Tested Contingency Plans - Total	71	100%
High	2	100%
Moderate	69	100%
Low	0	0%
Not categorized	0	0%
Total # of Systems not Categorized	0	
Incidents Reported to USCERT	45	
Incidents Reported to Law Enforcement	15	
Total Number of Employees	17,003	
Employees that received IT security awareness training	16,571	97%
Employees that received IT security awareness training using ISSLOB	0	
Total Number of Employees w/significant IT security responsibilities	636	
Employees with significant responsibilities that received training	579	91%
Total Costs for providing IT security training	$370,735	
The agency explains policies regarding peer-to-peer file sharing in training	Yes	
There is an agency-wide security configuration policy	Yes	
The agency applies common security configuration established by NIST to application information systems	Mostly (81-95% of the time)	
The agency has documented in its security policies special procedures for using emerging technologies and countering emerging threats	Yes	

Department of Labor -- IG Report

Quality of agency C&A process	Satisfactory
The Agency performs oversight and evaluation to ensure information systems used or operated by a contractor of the agency or other organization on behalf of the agency meet the requirements of FISMA, OMB Policy and NIST guidance	Rarely (0-50% of the time)
The agency has developed an inventory of major information systems, including an identification of interfaces (including those not under control of the agency)	The inventory is approximately 96-100% complete
The OIG generally agrees with the CIO on the number of agency owned systems	Yes
The OIG generally agrees with the CIO on the number of information systems used or operated by a contractor of the agency or other organization on behalf of the agency	Yes
The agency inventory is maintained and updated at least annually	Yes
The POA&M is an agency wide process, incorporating all known IT Security weaknesses associated with information systems used or operated by the agency or by a contractor of the agency or other organization on behalf of the agency	Frequently (71-80% of the time)
OIG Findings are incorporated into the POA&M process	Almost Always (96-100% of the time)
Effective POA&M process	Yes
There is an agency wide security configuration policy	Yes
The agency follows documented policies and procedures for identifying and reporting incidents internally	No
The agency follows documented policies and procedures for external reporting to law enforcement authorities	Yes
The agency follows defined procedures for reporting to the USCERT	Yes
The agency has ensured security training and awareness of all employees, including contractors with significant IT security responsibilities	Almost Always (96-100% of employees)
The agency explains policies regarding peer-to-peer file sharing in IT security awareness training, ethics training, or any other agency-wide training	Yes
Quality of the agency's PIA process, as discussed in Section D 11.4 (SAOP template), including adherence to existing policy, guidance and standards	Unaudited
The agency has completed system e-authentication risk assessments	No

Department of Labor -- Privacy Report

Systems that contain Federal information in identifiable form	187	
Agency	171	
Contractor	16	
Systems requiring a Privacy Impact Assessment under the E-Gov Act	43	
Agency	35	
Contractor	8	
Systems covered by an existing Privacy Impact Assessment	43	100%
Agency	35	
Contractor	8	
Systems for which a system or records notice (SORN) is required under the Privacy Act	156	
Agency	144	
Contractor	12	
Systems for which a current SORN has been published in the Federal Register	149	96%
Agency	137	
Contractor	12	
The privacy official participates in all agency information privacy compliance activities	Yes	
The privacy official participates in evaluating the ramifications for privacy of legislative, regulatory and other policy proposals, as well as testimony and comments under Circular A-19	Yes	
The privacy official participates in assessing the impact of technology on the privacy of personal information	Yes	
The agency has a training program to ensure all agency personnel and contractors with access to Federal data are generally familiar with information privacy laws, regulations and policies and understand the ramifications of inappropriate access and disclosure?	Yes	
The agency has a program for job-specific information privacy training for individuals involved in the administration of personal information or information technology systems, or with significant information security responsibilities	Yes	
The agency has written processes or policies for all listed aspects of Privacy Impact Assessments	Yes	
The agency has written process for determining continued compliance with stated web privacy policies	Yes	
Agency uses persistent tracking technology on any web site	No	
Agency annually reviews the use of persistent tracking	No	
Agency has current documentation demonstrating review of compliance with information privacy laws, regulations and policies	Yes	
Agency can provide documentation demonstrating corrective action planned, in progress, or completed to remedy identified compliance deficiencies	Yes	
Agency uses technologies that allow for continuous auditing of compliance with stated privacy policies and practices	Yes	
Agency coordinates with OIG on privacy program oversight	Yes	

-This page left blank intentionally-

National Aeronautics and Space Administration -- CIO Report

Total Number of Systems	809	
Agency Systems	760	
High	62	
Moderate	298	
Low	400	
Not categorized	0	
Contractor Systems	49	
High	2	
Moderate	34	
Low	11	
Not categorized	2	
Certified and Accredited Systems - Total	768	95%
High	63	98%
Moderate	305	92%
Low	400	97%
Not categorized	0	0%
Tested Security Controls - Total	778	96%
High	63	98%
Moderate	314	95%
Low	401	98%
Not categorized	0	0%
Tested Contingency Plans - Total	772	95%
High	63	98%
Moderate	309	93%
Low	400	97%
Not categorized	0	0%
Total # of Systems not Categorized	2	
Incidents Reported to USCERT	198	
Incidents Reported to Law Enforcement	198	
Total Number of Employees	55,538	
Employees that received IT security awareness training	52,385	94%
Employees that received IT security awareness training using ISSLOB	0	
Total Number of Employees w/significant IT security responsibilities	2,755	
Employees with significant responsibilities that received training	2,744	100%
Total Costs for providing IT security training	$1,200,000	
The agency explains policies regarding peer-to-peer file sharing in training	Yes	
There is an agency-wide security configuration policy	Yes	
The agency applies common security configuration established by NIST to application information systems	Mostly (81-95% of the time)	
The agency has documented in its security policies special procedures for using emerging technologies and countering emerging threats	Yes	

National Aeronautics and Space Administration -- IG Report

Quality of agency C&A process	Good
The Agency performs oversight and evaluation to ensure information systems used or operated by a contractor of the agency or other organization on behalf of the agency meet the requirements of FISMA, OMB Policy and NIST guidance	Sometimes (51-70% of the time)
The agency has developed an inventory of major information systems, including an identification of interfaces (including those not under control of the agency)	The inventory is approximately 96-100% complete
The OIG generally agrees with the CIO on the number of agency owned systems	Yes
The OIG generally agrees with the CIO on the number of information systems used or operated by a contractor of the agency or other organization on behalf of the agency	Yes
The agency inventory is maintained and updated at least annually	Yes
The POA&M is an agency wide process, incorporating all known IT Security weaknesses associated with information systems used or operated by the agency or by a contractor of the agency or other organization on behalf of the agency	Sometimes (51-70% of the time)
OIG Findings are incorporated into the POA&M process	Sometimes (51-70% of the time)
Effective POA&M process	No
There is an agency wide security configuration policy	Yes
The agency follows documented policies and procedures for identifying and reporting incidents internally	Yes
The agency follows documented policies and procedures for external reporting to law enforcement authorities	Yes
The agency follows defined procedures for reporting to the USCERT	Yes
The agency has ensured security training and awareness of all employees, including contractors with significant IT security responsibilities	Mostly (81-95% of employees)
The agency explains policies regarding peer-to-peer file sharing in IT security awareness training, ethics training, or any other agency-wide training	Yes
Quality of the agency's PIA process, as discussed in Section D 11.4 (SAOP template), including adherence to existing policy, guidance and standards	Good
The agency has completed system e-authentication risk assessments	Yes

National Aeronautics and Space Administration -- Privacy Report

Systems that contain Federal information in identifiable form	57	
Agency	15	
Contractor	42	
Systems requiring a Privacy Impact Assessment under the E-Gov Act	17	
Agency	6	
Contractor	11	
Systems covered by an existing Privacy Impact Assessment	17	100%
Agency	6	
Contractor	11	
Systems for which a system or records notice (SORN) is required under the Privacy Act	22	
Agency	12	
Contractor	10	
Systems for which a current SORN has been published in the Federal Register	20	91%
Agency	10	
Contractor	10	
The privacy official participates in all agency information privacy compliance activities	Yes	
The privacy official participates in evaluating the ramifications for privacy of legislative, regulatory and other policy proposals, as well as testimony and comments under Circular A-19	Yes	
The privacy official participates in assessing the impact of technology on the privacy of personal information	Yes	
The agency has a training program to ensure all agency personnel and contractors with access to Federal data are generally familiar with information privacy laws, regulations and policies and understand the ramifications of inappropriate access and disclosure?	Yes	
The agency has a program for job-specific information privacy training for individuals involved in the administration of personal information or information technology systems, or with significant information security responsibilities	Yes	
The agency has written processes or policies for all listed aspects of Privacy Impact Assessments	No	
The agency has written process for determining continued compliance with stated web privacy policies	Yes	
Agency uses persistent tracking technology on any web site	Yes	
Agency annually reviews the use of persistent tracking	Yes	
Agency has current documentation demonstrating review of compliance with information privacy laws, regulations and policies	Yes	
Agency can provide documentation demonstrating corrective action planned, in progress, or completed to remedy identified compliance deficiencies	Yes	
Agency uses technologies that allow for continuous auditing of compliance with stated privacy policies and practices	Yes	
Agency coordinates with OIG on privacy program oversight	Yes	

-This page left blank intentionally-

National Science Foundation -- CIO Report

Total Number of Systems	19	
Agency Systems	16	
High	4	
Moderate	8	
Low	4	
Not categorized	0	
Contractor Systems	3	
High	2	
Moderate	1	
Low	0	
Not categorized	0	
Certified and Accredited Systems - Total	19	100%
High	6	100%
Moderate	9	100%
Low	4	100%
Not categorized	0	0%
Tested Security Controls - Total	19	100%
High	6	100%
Moderate	9	100%
Low	4	100%
Not categorized	0	0%
Tested Contingency Plans - Total	19	100%
High	6	100%
Moderate	9	100%
Low	4	100%
Not categorized	0	0%
Total # of Systems not Categorized	0	
Incidents Reported to USCERT	4	
Incidents Reported to Law Enforcement	0	
Total Number of Employees	4,736	
Employees that received IT security awareness training	4,579	97%
Employees that received IT security awareness training using ISSLOB	0	
Total Number of Employees w/significant IT security responsibilities	85	
Employees with significant responsibilities that received training	85	100%
Total Costs for providing IT security training	$28,410	
The agency explains policies regarding peer-to-peer file sharing in training	Yes	
There is an agency-wide security configuration policy	Yes	
The agency applies common security configuration established by NIST to application information systems	Almost Always (96-100% of the time)	
The agency has documented in its security policies special procedures for using emerging technologies and countering emerging threats	Yes	

National Science Foundation -- IG Report

Quality of agency C&A process	Good
The Agency performs oversight and evaluation to ensure information systems used or operated by a contractor of the agency or other organization on behalf of the agency meet the requirements of FISMA, OMB Policy and NIST guidance	Almost Always (96-100% of the time)
The agency has developed an inventory of major information systems, including an identification of interfaces (including those not under control of the agency)	The inventory is approximately 96-100% complete
The OIG generally agrees with the CIO on the number of agency owned systems	Yes
The OIG generally agrees with the CIO on the number of information systems used or operated by a contractor of the agency or other organization on behalf of the agency	Yes
The agency inventory is maintained and updated at least annually	Yes
The POA&M is an agency wide process, incorporating all known IT Security weaknesses associated with information systems used or operated by the agency or by a contractor of the agency or other organization on behalf of the agency	Almost Always (96-100% of the time)
OIG Findings are incorporated into the POA&M process	Almost Always (96-100% of the time)
Effective POA&M process	Yes
There is an agency wide security configuration policy	Yes
The agency follows documented policies and procedures for identifying and reporting incidents internally	Yes
The agency follows documented policies and procedures for external reporting to law enforcement authorities	Yes
The agency follows defined procedures for reporting to the USCERT	Yes
The agency has ensured security training and awareness of all employees, including contractors with significant IT security responsibilities	Mostly (81-95% of employees)
The agency explains policies regarding peer-to-peer file sharing in IT security awareness training, ethics training, or any other agency-wide training	Yes
Quality of the agency's PIA process, as discussed in Section D 11.4 (SAOP template), including adherence to existing policy, guidance and standards	Excellent
The agency has completed system e-authentication risk assessments	Yes

National Science Foundation -- Privacy Report

Systems that contain Federal information in identifiable form	2	
Agency	2	
Contractor	0	
Systems requiring a Privacy Impact Assessment under the E-Gov Act	2	
Agency	2	
Contractor	0	
Systems covered by an existing Privacy Impact Assessment	2	100%
Agency	2	
Contractor	0	
Systems for which a system or records notice (SORN) is required under the Privacy Act	2	
Agency	2	
Contractor	0	
Systems for which a current SORN has been published in the Federal Register	2	100%
Agency	2	
Contractor	0	
The privacy official participates in all agency information privacy compliance activities	Yes	
The privacy official participates in evaluating the ramifications for privacy of legislative, regulatory and other policy proposals, as well as testimony and comments under Circular A-19	Yes	
The privacy official participates in assessing the impact of technology on the privacy of personal information	Yes	
The agency has a training program to ensure all agency personnel and contractors with access to Federal data are generally familiar with information privacy laws, regulations and policies and understand the ramifications of inappropriate access and disclosure?	Yes	
The agency has a program for job-specific information privacy training for individuals involved in the administration of personal information or information technology systems, or with significant information security responsibilities	Yes	
The agency has written processes or policies for all listed aspects of Privacy Impact Assessments	Yes	
The agency has written process for determining continued compliance with stated web privacy policies	Yes	
Agency uses persistent tracking technology on any web site	No	
Agency annually reviews the use of persistent tracking	No	
Agency has current documentation demonstrating review of compliance with information privacy laws, regulations and policies	Yes	
Agency can provide documentation demonstrating corrective action planned, in progress, or completed to remedy identified compliance deficiencies	Yes	
Agency uses technologies that allow for continuous auditing of compliance with stated privacy policies and practices	Yes	
Agency coordinates with OIG on privacy program oversight	Yes	

-This page left blank intentionally-

Nuclear Regulatory Commission -- CIO Report

Total Number of Systems	42	
Agency Systems	31	
High	4	
Moderate	11	
Low	0	
Not categorized	16	
Contractor Systems	11	
High	0	
Moderate	4	
Low	1	
Not categorized	6	
Certified and Accredited Systems - Total	7	17%
High	1	25%
Moderate	5	33%
Low	1	100%
Not categorized	0	0%
Tested Security Controls - Total	36	86%
High	4	100%
Moderate	13	87%
Low	1	100%
Not categorized	18	82%
Tested Contingency Plans - Total	7	17%
High	0	0%
Moderate	7	47%
Low	0	0%
Not categorized	0	0%
Total # of Systems not Categorized	22	
Incidents Reported to USCERT	9	
Incidents Reported to Law Enforcement	0	
Total Number of Employees	3,749	
Employees that received IT security awareness training	3,749	100%
Employees that received IT security awareness training using ISSLOB	0	
Total Number of Employees w/significant IT security responsibilities	118	
Employees with significant responsibilities that received training	11	9%
Total Costs for providing IT security training	$332,000	
The agency explains policies regarding peer-to-peer file sharing in training	Yes	
There is an agency-wide security configuration policy	Yes	
The agency applies common security configuration established by NIST to application information systems	Rarely (0-50% of the time)	
The agency has documented in its security policies special procedures for using emerging technologies and countering emerging threats	Yes	

Nuclear Regulatory Commission -- IG Report

Quality of agency C&A process	Failing
The Agency performs oversight and evaluation to ensure information systems used or operated by a contractor of the agency or other organization on behalf of the agency meet the requirements of FISMA, OMB Policy and NIST guidance	Mostly (81-95% of the time)
The agency has developed an inventory of major information systems, including an identification of interfaces (including those not under control of the agency)	The inventory is approximately 81-95% complete
The OIG generally agrees with the CIO on the number of agency owned systems	Yes
The OIG generally agrees with the CIO on the number of information systems used or operated by a contractor of the agency or other organization on behalf of the agency	Yes
The agency inventory is maintained and updated at least annually	Yes
The POA&M is an agency wide process, incorporating all known IT Security weaknesses associated with information systems used or operated by the agency or by a contractor of the agency or other organization on behalf of the agency	Almost Always (96-100% of the time)
OIG Findings are incorporated into the POA&M process	Almost Always (96-100% of the time)
Effective POA&M process	Yes
There is an agency wide security configuration policy	Yes
The agency follows documented policies and procedures for identifying and reporting incidents internally	Yes
The agency follows documented policies and procedures for external reporting to law enforcement authorities	Yes
The agency follows defined procedures for reporting to the USCERT	Yes
The agency has ensured security training and awareness of all employees, including contractors with significant IT security responsibilities	Almost Always(96-100% of employees)
The agency explains policies regarding peer-to-peer file sharing in IT security awareness training, ethics training, or any other agency-wide training	Yes
Quality of the agency's PIA process, as discussed in Section D 11.4 (SAOP template), including adherence to existing policy, guidance and standards	Excellent
The agency has completed system e-authentication risk assessments	No

Nuclear Regulatory Commission -- Privacy Report

Systems that contain Federal information in identifiable form	68	
Agency	59	
Contractor	9	
Systems requiring a Privacy Impact Assessment under the E-Gov Act	25	
Agency	18	
Contractor	7	
Systems covered by an existing Privacy Impact Assessment	11	44%
Agency	7	
Contractor	4	
Systems for which a system or records notice (SORN) is required under the Privacy Act	40	
Agency	33	
Contractor	7	
Systems for which a current SORN has been published in the Federal Register	40	100%
Agency	33	
Contractor	7	
The privacy official participates in all agency information privacy compliance activities	Yes	
The privacy official participates in evaluating the ramifications for privacy of legislative, regulatory and other policy proposals, as well as testimony and comments under Circular A-19	No	
The privacy official participates in assessing the impact of technology on the privacy of personal information	Yes	
The agency has a training program to ensure all agency personnel and contractors with access to Federal data are generally familiar with information privacy laws, regulations and policies and understand the ramifications of inappropriate access and disclosure?	Yes	
The agency has a program for job-specific information privacy training for individuals involved in the administration of personal information or information technology systems, or with significant information security responsibilities	Yes	
The agency has written processes or policies for all listed aspects of Privacy Impact Assessments	Yes	
The agency has written process for determining continued compliance with stated web privacy policies	Yes	
Agency uses persistent tracking technology on any web site	Yes	
Agency annually reviews the use of persistent tracking	No	
Agency has current documentation demonstrating review of compliance with information privacy laws, regulations and policies	Yes	
Agency can provide documentation demonstrating corrective action planned, in progress, or completed to remedy identified compliance deficiencies	Yes	
Agency uses technologies that allow for continuous auditing of compliance with stated privacy policies and practices	No	
Agency coordinates with OIG on privacy program oversight	Yes	

-This page left blank intentionally-

Office of Personnel Management -- CIO Report

Total Number of Systems	41	
Agency Systems	30	
High	5	
Moderate	25	
Low	0	
Not categorized	0	
Contractor Systems	11	
High	2	
Moderate	9	
Low	0	
Not categorized	0	
Certified and Accredited Systems - Total	41	100%
High	7	100%
Moderate	34	100%
Low	0	0%
Not categorized	0	0%
Tested Security Controls - Total	41	100%
High	7	100%
Moderate	34	100%
Low	0	0%
Not categorized	0	0%
Tested Contingency Plans - Total	41	100%
High	7	100%
Moderate	34	100%
Low	0	0%
Not categorized	0	0%
Total # of Systems not Categorized	0	
Incidents Reported to USCERT	70	
Incidents Reported to Law Enforcement	1	
Total Number of Employees	5,871	
Employees that received IT security awareness training	5,871	100%
Employees that received IT security awareness training using ISSLOB	5,871	
Total Number of Employees w/significant IT security responsibilities	107	
Employees with significant responsibilities that received training	107	100%
Total Costs for providing IT security training	$47,200	
The agency explains policies regarding peer-to-peer file sharing in training	Yes	
There is an agency-wide security configuration policy	Yes	
The agency applies common security configuration established by NIST to application information systems	Almost Always (96-100% of the time)	
The agency has documented in its security policies special procedures for using emerging technologies and countering emerging threats	Yes	

Office of Personnel Management -- IG Report

Quality of agency C&A process	Excellent
The Agency performs oversight and evaluation to ensure information systems used or operated by a contractor of the agency or other organization on behalf of the agency meet the requirements of FISMA, OMB Policy and NIST guidance	Almost Always (96-100% of the time)
The agency has developed an inventory of major information systems, including an identification of interfaces (including those not under control of the agency)	The inventory is approximately 96-100% complete
The OIG generally agrees with the CIO on the number of agency owned systems	Yes
The OIG generally agrees with the CIO on the number of information systems used or operated by a contractor of the agency or other organization on behalf of the agency	Yes
The agency inventory is maintained and updated at least annually	Yes
The POA&M is an agency wide process, incorporating all known IT Security weaknesses associated with information systems used or operated by the agency or by a contractor of the agency or other organization on behalf of the agency	Almost Always (96-100% of the time)
OIG Findings are incorporated into the POA&M process	Almost Always (96-100% of the time)
Effective POA&M process	Yes
There is an agency wide security configuration policy	Yes
The agency follows documented policies and procedures for identifying and reporting incidents internally	No
The agency follows documented policies and procedures for external reporting to law enforcement authorities	Yes
The agency follows defined procedures for reporting to the USCERT	Yes
The agency has ensured security training and awareness of all employees, including contractors with significant IT security responsibilities	Almost Always(96-100% of employees)
The agency explains policies regarding peer-to-peer file sharing in IT security awareness training, ethics training, or any other agency-wide training	Yes
Quality of the agency's PIA process, as discussed in Section D 11.4 (SAOP template), including adherence to existing policy, guidance and standards	Satisfactory
The agency has completed system e-authentication risk assessments	Yes

Office of Personnel Management-- Privacy Report

Systems that contain Federal information in identifiable form	37	
Agency	27	
Contractor	10	
Systems requiring a Privacy Impact Assessment under the E-Gov Act	25	
Agency	18	
Contractor	7	
Systems covered by an existing Privacy Impact Assessment	5	20%
Agency	4	
Contractor	1	
Systems for which a system or records notice (SORN) is required under the Privacy Act	36	
Agency	25	
Contractor	11	
Systems for which a current SORN has been published in the Federal Register	36	100%
Agency	25	
Contractor	11	
The privacy official participates in all agency information privacy compliance activities	Yes	
The privacy official participates in evaluating the ramifications for privacy of legislative, regulatory and other policy proposals, as well as testimony and comments under Circular A-19	Yes	
The privacy official participates in assessing the impact of technology on the privacy of personal information	Yes	
The agency has a training program to ensure all agency personnel and contractors with access to Federal data are generally familiar with information privacy laws, regulations and policies and understand the ramifications of inappropriate access and disclosure?	Yes	
The agency has a program for job-specific information privacy training for individuals involved in the administration of personal information or information technology systems, or with significant information security responsibilities	Yes	
The agency has written processes or policies for all listed aspects of Privacy Impact Assessments	Yes	
The agency has written process for determining continued compliance with stated web privacy policies	Yes	
Agency uses persistent tracking technology on any web site	No	
Agency annually reviews the use of persistent tracking	Yes	
Agency has current documentation demonstrating review of compliance with information privacy laws, regulations and policies	Yes	
Agency can provide documentation demonstrating corrective action planned, in progress, or completed to remedy identified compliance deficiencies	Yes	
Agency uses technologies that allow for continuous auditing of compliance with stated privacy policies and practices	Yes	
Agency coordinates with OIG on privacy program oversight	Yes	

-This page left blank intentionally-

Small Business Administration -- CIO Report

Total Number of Systems	87	
Agency Systems	78	
High	4	
Moderate	14	
Low	60	
Not categorized	0	
Contractor Systems	9	
High	2	
Moderate	7	
Low	0	
Not categorized	0	
Certified and Accredited Systems - Total	87	100%
High	6	100%
Moderate	21	100%
Low	60	100%
Not categorized	0	0%
Tested Security Controls - Total	86	99%
High	6	100%
Moderate	20	95%
Low	60	100%
Not categorized	0	0%
Tested Contingency Plans - Total	86	99%
High	6	100%
Moderate	20	95%
Low	60	100%
Not categorized	0	0%
Total # of Systems not Categorized	0	
Incidents Reported to USCERT	1	
Incidents Reported to Law Enforcement	0	
Total Number of Employees	5,298	
Employees that received IT security awareness training	3,416	64%
Employees that received IT security awareness training using ISSLOB	0	
Total Number of Employees w/significant IT security responsibilities	75	
Employees with significant responsibilities that received training	75	100%
Total Costs for providing IT security training	$65,000	
The agency explains policies regarding peer-to-peer file sharing in training	Yes	
There is an agency-wide security configuration policy	Yes	
The agency applies common security configuration established by NIST to application information systems	Almost Always (96-100% of the time)	
The agency has documented in its security policies special procedures for using emerging technologies and countering emerging threats	Yes	

Small Business Administration -- IG Report

Quality of agency C&A process	Satisfactory
The Agency performs oversight and evaluation to ensure information systems used or operated by a contractor of the agency or other organization on behalf of the agency meet the requirements of FISMA, OMB Policy and NIST guidance	Frequently 71-80% of the time)
The agency has developed an inventory of major information systems, including an identification of interfaces (including those not under control of the agency)	The inventory is approximately 96-100% complete
The OIG generally agrees with the CIO on the number of agency owned systems	Yes
The OIG generally agrees with the CIO on the number of information systems used or operated by a contractor of the agency or other organization on behalf of the agency	Yes
The agency inventory is maintained and updated at least annually	Yes
The POA&M is an agency wide process, incorporating all known IT Security weaknesses associated with information systems used or operated by the agency or by a contractor of the agency or other organization on behalf of the agency	Almost Always (96-100% of the time)
OIG Findings are incorporated into the POA&M process	Almost Always (96-100% of the time)
Effective POA&M process	Yes
There is an agency wide security configuration policy	Yes
The agency follows documented policies and procedures for identifying and reporting incidents internally	Yes
The agency follows documented policies and procedures for external reporting to law enforcement authorities	Yes
The agency follows defined procedures for reporting to the USCERT	Yes
The agency has ensured security training and awareness of all employees, including contractors with significant IT security responsibilities	Sometimes (51-70% of employees)
The agency explains policies regarding peer-to-peer file sharing in IT security awareness training, ethics training, or any other agency-wide training	Yes
Quality of the agency's PIA process, as discussed in Section D 11.4 (SAOP template), including adherence to existing policy, guidance and standards	Satisfactory
The agency has completed system e-authentication risk assessments	Yes

Small Business Administration -- Privacy Report

Systems that contain Federal information in identifiable form	24	
Agency	21	
Contractor	3	
Systems requiring a Privacy Impact Assessment under the E-Gov Act	24	
Agency	21	
Contractor	3	
Systems covered by an existing Privacy Impact Assessment	23	96%
Agency	20	
Contractor	3	
Systems for which a system or records notice (SORN) is required under the Privacy Act	23	
Agency	20	
Contractor	3	
Systems for which a current SORN has been published in the Federal Register	23	100%
Agency	20	
Contractor	3	
The privacy official participates in all agency information privacy compliance activities	Yes	
The privacy official participates in evaluating the ramifications for privacy of legislative, regulatory and other policy proposals, as well as testimony and comments under Circular A-19	Yes	
The privacy official participates in assessing the impact of technology on the privacy of personal information	Yes	
The agency has a training program to ensure all agency personnel and contractors with access to Federal data are generally familiar with information privacy laws, regulations and policies and understand the ramifications of inappropriate access and disclosure?	Yes	
The agency has a program for job-specific information privacy training for individuals involved in the administration of personal information or information technology systems, or with significant information security responsibilities	Yes	
The agency has written processes or policies for all listed aspects of Privacy Impact Assessments	Yes	
The agency has written process for determining continued compliance with stated web privacy policies	No	
Agency uses persistent tracking technology on any web site	No	
Agency annually reviews the use of persistent tracking	No	
Agency has current documentation demonstrating review of compliance with information privacy laws, regulations and policies	Yes	
Agency can provide documentation demonstrating corrective action planned, in progress, or completed to remedy identified compliance deficiencies	Yes	
Agency uses technologies that allow for continuous auditing of compliance with stated privacy policies and practices	Yes	
Agency coordinates with OIG on privacy program oversight	Yes	

-This page left blank intentionally-

Smithsonian Institution -- CIO Report

Total Number of Systems	15	
Agency Systems	14	
High	0	
Moderate	7	
Low	7	
Not categorized	0	
Contractor Systems	1	
High	0	
Moderate	1	
Low	0	
Not categorized	0	
Certified and Accredited Systems - Total	15	100%
High	0	0%
Moderate	8	100%
Low	7	100%
Not categorized	0	0%
Tested Security Controls - Total	15	100%
High	0	0%
Moderate	8	100%
Low	7	100%
Not categorized	0	0%
Tested Contingency Plans - Total	15	100%
High	0	0%
Moderate	8	100%
Low	7	100%
Not categorized	0	0%
Total # of Systems not Categorized	0	
Incidents Reported to USCERT	4	
Incidents Reported to Law Enforcement	0	
Total Number of Employees	7,705	
Employees that received IT security awareness training	7,701	100%
Employees that received IT security awareness training using ISSLOB	0	
Total Number of Employees w/significant IT security responsibilities	152	
Employees with significant responsibilities that received training	34	22%
Total Costs for providing IT security training	$47,066	
The agency explains policies regarding peer-to-peer file sharing in training	Yes	
There is an agency-wide security configuration policy	Yes	
The agency applies common security configuration established by NIST to application information systems	Mostly	
The agency has documented in its security policies special procedures for using emerging technologies and countering emerging threats	Yes	

Smithsonian Institution -- IG Report

Quality of agency C&A process	Satisfactory
The Agency performs oversight and evaluation to ensure information systems used or operated by a contractor of the agency or other organization on behalf of the agency meet the requirements of FISMA, OMB Policy and NIST guidance	Almost Always (96-100% of the time)
The agency has developed an inventory of major information systems, including an identification of interfaces (including those not under control of the agency)	The inventory is approximately 81-95% complete
The OIG generally agrees with the CIO on the number of agency owned systems	Yes
The OIG generally agrees with the CIO on the number of information systems used or operated by a contractor of the agency or other organization on behalf of the agency	No
The agency inventory is maintained and updated at least annually	Yes
The POA&M is an agency wide process, incorporating all known IT Security weaknesses associated with information systems used or operated by the agency or by a contractor of the agency or other organization on behalf of the agency	Frequently (71-80% of the time)
OIG Findings are incorporated into the POA&M process	Almost Always (96-100% of the time)
Effective POA&M process	Yes*
There is an agency wide security configuration policy	Yes
The agency follows documented policies and procedures for identifying and reporting incidents internally	Yes
The agency follows documented policies and procedures for external reporting to law enforcement authorities	Yes
The agency follows defined procedures for reporting to the USCERT	Yes
The agency has ensured security training and awareness of all employees, including contractors with significant IT security responsibilities	Frequently (71-80% of employees)
The agency explains policies regarding peer-to-peer file sharing in IT security awareness training, ethics training, or any other agency-wide training	Yes
Quality of the agency's PIA process, as discussed in Section D 11.4 (SAOP template), including adherence to existing policy, guidance and standards	Good
The agency has completed system e-authentication risk assessments	Yes

* Effective POA&M determined by Agency Head.

Smithsonian Institution -- Privacy Report

Systems that contain Federal information in identifiable form	13	
Agency	12	
Contractor	1	
Systems requiring a Privacy Impact Assessment under the E-Gov Act	12	
Agency	11	
Contractor	1	
Systems covered by an existing Privacy Impact Assessment	12	100%
Agency	11	
Contractor	1	
Systems for which a system or records notice (SORN) is required under the Privacy Act	0	
Agency	0	
Contractor	0	
Systems for which a current SORN has been published in the Federal Register	0	0%
Agency	0	
Contractor	0	
The privacy official participates in all agency information privacy compliance activities	Yes	
The privacy official participates in evaluating the ramifications for privacy of legislative, regulatory and other policy proposals, as well as testimony and comments under Circular A-19	Yes	
The privacy official participates in assessing the impact of technology on the privacy of personal information	Yes	
The agency has a training program to ensure all agency personnel and contractors with access to Federal data are generally familiar with information privacy laws, regulations and policies and understand the ramifications of inappropriate access and disclosure?	Yes	
The agency has a program for job-specific information privacy training for individuals involved in the administration of personal information or information technology systems, or with significant information security responsibilities	Yes	
The agency has written processes or policies for all listed aspects of Privacy Impact Assessments	Yes	
The agency has written process for determining continued compliance with stated web privacy policies	Yes	
Agency uses persistent tracking technology on any web site	Yes	
Agency annually reviews the use of persistent tracking	Yes	
Agency has current documentation demonstrating review of compliance with information privacy laws, regulations and policies	Yes	
Agency can provide documentation demonstrating corrective action planned, in progress, or completed to remedy identified compliance deficiencies	Yes	
Agency uses technologies that allow for continuous auditing of compliance with stated privacy policies and practices	Yes	
Agency coordinates with OIG on privacy program oversight	Yes	

-This page left blank intentionally-

Social Security Administration -- CIO Report

Total Number of Systems	20	
Agency Systems	20	
High	0	
Moderate	8	
Low	12	
Not categorized	0	
Contractor Systems	0	
High	0	
Moderate	0	
Low	0	
Not categorized	0	
Certified and Accredited Systems - Total	20	100%
High	0	0%
Moderate	8	100%
Low	12	100%
Not categorized	0	0%
Tested Security Controls - Total	20	100%
High	0	0%
Moderate	8	100%
Low	12	100%
Not categorized	0	0%
Tested Contingency Plans - Total	20	100%
High	0	0%
Moderate	8	100%
Low	12	100%
Not categorized	0	0%
Total # of Systems not Categorized	0	
Incidents Reported to USCERT	111	
Incidents Reported to Law Enforcement	8	
Total Number of Employees	64,170	
Employees that received IT security awareness training	64,170	100%
Employees that received IT security awareness training using ISSLOB	623	
Total Number of Employees w/significant IT security responsibilities	339	
Employees with significant responsibilities that received training	339	100%
Total Costs for providing IT security training	$1,376,196	
The agency explains policies regarding peer-to-peer file sharing in training	Yes	
There is an agency-wide security configuration policy	Yes	
The agency applies common security configuration established by NIST to application information systems	Almost Always (96-100% of the time)	
The agency has documented in its security policies special procedures for using emerging technologies and countering emerging threats	Yes	

Social Security Administration -- IG Report

Quality of agency C&A process	Excellent
The Agency performs oversight and evaluation to ensure information systems used or operated by a contractor of the agency or other organization on behalf of the agency meet the requirements of FISMA, OMB Policy and NIST guidance	n/a
The agency has developed an inventory of major information systems, including an identification of interfaces (including those not under control of the agency)	The inventory is approximately 96-100% complete
The OIG generally agrees with the CIO on the number of agency owned systems	Yes
The OIG generally agrees with the CIO on the number of information systems used or operated by a contractor of the agency or other organization on behalf of the agency	Yes
The agency inventory is maintained and updated at least annually	Yes
The POA&M is an agency wide process, incorporating all known IT Security weaknesses associated with information systems used or operated by the agency or by a contractor of the agency or other organization on behalf of the agency	Almost Always (96-100% of the time)
OIG Findings are incorporated into the POA&M process	Almost Always (96-100% of the time)
Effective POA&M process	Yes
There is an agency wide security configuration policy	Yes
The agency follows documented policies and procedures for identifying and reporting incidents internally	Yes
The agency follows documented policies and procedures for external reporting to law enforcement authorities	Yes
The agency follows defined procedures for reporting to the USCERT	Yes
The agency has ensured security training and awareness of all employees, including contractors with significant IT security responsibilities	Frequently (71-80% of employees)
The agency explains policies regarding peer-to-peer file sharing in IT security awareness training, ethics training, or any other agency-wide training	Yes
Quality of the agency's PIA process, as discussed in Section D 11.4 (SAOP template), including adherence to existing policy, guidance and standards	Good
The agency has completed system e-authentication risk assessments	Yes

Social Security Administration -- Privacy Report

Systems that contain Federal information in identifiable form	19	
Agency	19	
Contractor	0	
Systems requiring a Privacy Impact Assessment under the E-Gov Act	16	
Agency	16	
Contractor	0	
Systems covered by an existing Privacy Impact Assessment	16	100%
Agency	16	
Contractor	0	
Systems for which a system or records notice (SORN) is required under the Privacy Act	18	
Agency	18	
Contractor	0	
Systems for which a current SORN has been published in the Federal Register	18	100%
Agency	18	
Contractor	0	
The privacy official participates in all agency information privacy compliance activities	Yes	
The privacy official participates in evaluating the ramifications for privacy of legislative, regulatory and other policy proposals, as well as testimony and comments under Circular A-19	Yes	
The privacy official participates in assessing the impact of technology on the privacy of personal information	Yes	
The agency has a training program to ensure all agency personnel and contractors with access to Federal data are generally familiar with information privacy laws, regulations and policies and understand the ramifications of inappropriate access and disclosure?	Yes	
The agency has a program for job-specific information privacy training for individuals involved in the administration of personal information or information technology systems, or with significant information security responsibilities	Yes	
The agency has written processes or policies for all listed aspects of Privacy Impact Assessments	Yes	
The agency has written process for determining continued compliance with stated web privacy policies	Yes	
Agency uses persistent tracking technology on any web site	No	
Agency annually reviews the use of persistent tracking	Yes	
Agency has current documentation demonstrating review of compliance with information privacy laws, regulations and policies	Yes	
Agency can provide documentation demonstrating corrective action planned, in progress, or completed to remedy identified compliance deficiencies	Yes	
Agency uses technologies that allow for continuous auditing of compliance with stated privacy policies and practices	Yes	
Agency coordinates with OIG on privacy program oversight	Yes	

-This page left blank intentionally-

Department of State -- CIO Report

Total Number of Systems	347	
Agency Systems	222	
High	26	
Moderate	100	
Low	96	
Not categorized	0	
Contractor Systems	125	
High	0	
Moderate	26	
Low	99	
Not categorized	0	
Certified and Accredited Systems - Total	347	100%
High	26	100%
Moderate	126	100%
Low	195	100%
Not categorized	0	0%
Tested Security Controls - Total	347	100%
High	26	100%
Moderate	126	100%
Low	195	100%
Not categorized	0	0%
Tested Contingency Plans - Total	328	95%
High	22	85%
Moderate	112	89%
Low	194	99%
Not categorized	0	0%
Total # of Systems not Categorized	0	
Incidents Reported to USCERT	5	
Incidents Reported to Law Enforcement	5	
Total Number of Employees	57,096	
Employees that received IT security awareness training	56,757	99%
Employees that received IT security awareness training using ISSLOB	1,364	
Total Number of Employees w/significant IT security responsibilities	2,132	
Employees with significant responsibilities that received training	1,006	47%
Total Costs for providing IT security training	$3,200,000	
The agency explains policies regarding peer-to-peer file sharing in training	Yes	
There is an agency-wide security configuration policy	Yes	
The agency applies common security configuration established by NIST to application information systems	Almost Always (96-100% of the time)	
The agency has documented in its security policies special procedures for using emerging technologies and countering emerging threats	Yes	

Department of State -- IG Report

Quality of agency C&A process	Satisfactory
The Agency performs oversight and evaluation to ensure information systems used or operated by a contractor of the agency or other organization on behalf of the agency meet the requirements of FISMA, OMB Policy and NIST guidance	Sometimes (51-70% of the time)
The agency has developed an inventory of major information systems, including an identification of interfaces (including those not under control of the agency)	The inventory is approximately 96-100% complete
The OIG generally agrees with the CIO on the number of agency owned systems	Yes
The OIG generally agrees with the CIO on the number of information systems used or operated by a contractor of the agency or other organization on behalf of the agency	Yes
The agency inventory is maintained and updated at least annually	Yes
The POA&M is an agency wide process, incorporating all known IT Security weaknesses associated with information systems used or operated by the agency or by a contractor of the agency or other organization on behalf of the agency	Mostly (81-95% of the time)
OIG Findings are incorporated into the POA&M process	Mostly (81-95% of the time)
Effective POA&M process	No
There is an agency wide security configuration policy	Yes
The agency follows documented policies and procedures for identifying and reporting incidents internally	Yes
The agency follows documented policies and procedures for external reporting to law enforcement authorities	Yes
The agency follows defined procedures for reporting to the USCERT	Yes
The agency has ensured security training and awareness of all employees, including contractors with significant IT security responsibilities	Frequently (71-80% of employees)
The agency explains policies regarding peer-to-peer file sharing in IT security awareness training, ethics training, or any other agency-wide training	Yes
Quality of the agency's PIA process, as discussed in Section D 11.4 (SAOP template), including adherence to existing policy, guidance and standards	Satisfactory
The agency has completed system e-authentication risk assessments	Yes

Department of State -- Privacy Report

Systems that contain Federal information in identifiable form	117	
Agency	91	
Contractor	26	
Systems requiring a Privacy Impact Assessment under the E-Gov Act	91	
Agency	91	
Contractor	0	
Systems covered by an existing Privacy Impact Assessment	85	93%
Agency	85	
Contractor	0	
Systems for which a system or records notice (SORN) is required under the Privacy Act	118	
Agency	95	
Contractor	23	
Systems for which a current SORN has been published in the Federal Register	118	100%
Agency	95	
Contractor	23	
The privacy official participates in all agency information privacy compliance activities	Yes	
The privacy official participates in evaluating the ramifications for privacy of legislative, regulatory and other policy proposals, as well as testimony and comments under Circular A-19	Yes	
The privacy official participates in assessing the impact of technology on the privacy of personal information	Yes	
The agency has a training program to ensure all agency personnel and contractors with access to Federal data are generally familiar with information privacy laws, regulations and policies and understand the ramifications of inappropriate access and disclosure?	Yes	
The agency has a program for job-specific information privacy training for individuals involved in the administration of personal information or information technology systems, or with significant information security responsibilities	Yes	
The agency has written processes or policies for all listed aspects of Privacy Impact Assessments	Yes	
The agency has written process for determining continued compliance with stated web privacy policies	Yes	
Agency uses persistent tracking technology on any web site	No	
Agency annually reviews the use of persistent tracking	Yes	
Agency has current documentation demonstrating review of compliance with information privacy laws, regulations and policies	Yes	
Agency can provide documentation demonstrating corrective action planned, in progress, or completed to remedy identified compliance deficiencies	Yes	
Agency uses technologies that allow for continuous auditing of compliance with stated privacy policies and practices	Yes	
Agency coordinates with OIG on privacy program oversight	Yes	

-This page left blank intentionally-

Department of Transportation -- CIO Report

Total Number of Systems	414	
Agency Systems	400	
High	29	
Moderate	257	
Low	114	
Not categorized	0	
Contractor Systems	14	
High	0	
Moderate	10	
Low	4	
Not categorized	0	
Certified and Accredited Systems - Total	393	95%
High	29	100%
Moderate	254	95%
Low	110	93%
Not categorized	0	0%
Tested Security Controls - Total	376	91%
High	24	83%
Moderate	244	91%
Low	108	92%
Not categorized	0	0%
Tested Contingency Plans - Total	349	84%
High	24	83%
Moderate	264	99%
Low	61	52%
Not categorized	0	0%
Total # of Systems not Categorized	0	
Incidents Reported to USCERT	381	
Incidents Reported to Law Enforcement	15	
Total Number of Employees	65,490	
Employees that received IT security awareness training	56,533	86%
Employees that received IT security awareness training using ISSLOB	0	
Total Number of Employees w/significant IT security responsibilities	1,077	
Employees with significant responsibilities that received training	994	92%
Total Costs for providing IT security training	$1,217,763	
The agency explains policies regarding peer-to-peer file sharing in training	Yes	
There is an agency-wide security configuration policy	Yes	
The agency applies common security configuration established by NIST to application information systems	Rarely (0-50% of the time)	
The agency has documented in its security policies special procedures for using emerging technologies and countering emerging threats	Yes	

Department of Transportation -- IG Report

Quality of agency C&A process	Satisfactory
The Agency performs oversight and evaluation to ensure information systems used or operated by a contractor of the agency or other organization on behalf of the agency meet the requirements of FISMA, OMB Policy and NIST guidance	Almost Always (96-100% of the time)
The agency has developed an inventory of major information systems, including an identification of interfaces (including those not under control of the agency)	The inventory is approximately 96-100% complete
The OIG generally agrees with the CIO on the number of agency owned systems	Yes
The OIG generally agrees with the CIO on the number of information systems used or operated by a contractor of the agency or other organization on behalf of the agency	Yes
The agency inventory is maintained and updated at least annually	Yes
The POA&M is an agency wide process, incorporating all known IT Security weaknesses associated with information systems used or operated by the agency or by a contractor of the agency or other organization on behalf of the agency	Sometimes (51-70% of the time)
OIG Findings are incorporated into the POA&M process	Almost Always (96-100% of the time)
Effective POA&M process	Yes
There is an agency wide security configuration policy	Yes
The agency follows documented policies and procedures for identifying and reporting incidents internally	Yes
The agency follows documented policies and procedures for external reporting to law enforcement authorities	Yes
The agency follows defined procedures for reporting to the USCERT	Yes
The agency has ensured security training and awareness of all employees, including contractors with significant IT security responsibilities	Frequently (71-80% of employees)
The agency explains policies regarding peer-to-peer file sharing in IT security awareness training, ethics training, or any other agency-wide training	Yes
Quality of the agency's PIA process, as discussed in Section D 11.4 (SAOP template), including adherence to existing policy, guidance and standards	Good
The agency has completed system e-authentication risk assessments	Yes

Department of Transportation -- Privacy Report

Systems that contain Federal information in identifiable form	309	
Agency	159	
Contractor	150	
Systems requiring a Privacy Impact Assessment under the E-Gov Act	151	
Agency	97	
Contractor	54	
Systems covered by an existing Privacy Impact Assessment	134	89%
Agency	92	
Contractor	42	
Systems for which a system or records notice (SORN) is required under the Privacy Act	230	
Agency	124	
Contractor	106	
Systems for which a current SORN has been published in the Federal Register	221	96%
Agency	119	
Contractor	102	
The privacy official participates in all agency information privacy compliance activities	Yes	
The privacy official participates in evaluating the ramifications for privacy of legislative, regulatory and other policy proposals, as well as testimony and comments under Circular A-19	Yes	
The privacy official participates in assessing the impact of technology on the privacy of personal information	Yes	
The agency has a training program to ensure all agency personnel and contractors with access to Federal data are generally familiar with information privacy laws, regulations and policies and understand the ramifications of inappropriate access and disclosure?	Yes	
The agency has a program for job-specific information privacy training for individuals involved in the administration of personal information or information technology systems, or with significant information security responsibilities	Yes	
The agency has written processes or policies for all listed aspects of Privacy Impact Assessments	Yes	
The agency has written process for determining continued compliance with stated web privacy policies	Yes	
Agency uses persistent tracking technology on any web site	No	
Agency annually reviews the use of persistent tracking	Yes	
Agency has current documentation demonstrating review of compliance with information privacy laws, regulations and policies	Yes	
Agency can provide documentation demonstrating corrective action planned, in progress, or completed to remedy identified compliance deficiencies	Yes	
Agency uses technologies that allow for continuous auditing of compliance with stated privacy policies and practices	Yes	
Agency coordinates with OIG on privacy program oversight	Yes	

-This page left blank intentionally-

Department of Treasury -- CIO Report

Total Number of Systems	585	
Agency Systems	557	
High	35	
Moderate	368	
Low	153	
Not categorized	1	
Contractor Systems	28	
High	5	
Moderate	21	
Low	2	
Not categorized	0	
Certified and Accredited Systems - Total	552	94%
High	39	98%
Moderate	365	94%
Low	148	95%
Not categorized	0	0%
Tested Security Controls - Total	544	93%
High	36	90%
Moderate	356	92%
Low	152	98%
Not categorized	0	0%
Tested Contingency Plans - Total	543	93%
High	35	88%
Moderate	355	91%
Low	153	99%
Not categorized	0	0%
Total # of Systems not Categorized	1	
Incidents Reported to USCERT	290	
Incidents Reported to Law Enforcement	99	
Total Number of Employees	115,011	
Employees that received IT security awareness training	111,952	97%
Employees that received IT security awareness training using ISSLOB	0	
Total Number of Employees w/significant IT security responsibilities	5,420	
Employees with significant responsibilities that received training	5,289	98%
Total Costs for providing IT security training	$5,542,774	
The agency explains policies regarding peer-to-peer file sharing in training	Yes	
There is an agency-wide security configuration policy	Yes	
The agency applies common security configuration established by NIST to application information systems	Frequently (71-80% of the time)	
The agency has documented in its security policies special procedures for using emerging technologies and countering emerging threats	Yes	

Department of Treasury -- IG Report

Quality of agency C&A process	Satisfactory
The Agency performs oversight and evaluation to ensure information systems used or operated by a contractor of the agency or other organization on behalf of the agency meet the requirements of FISMA, OMB Policy and NIST guidance	Almost Always (96-100% of the time)
The agency has developed an inventory of major information systems, including an identification of interfaces (including those not under control of the agency)	The inventory is approximately 51-70% complete
The OIG generally agrees with the CIO on the number of agency owned systems	Yes
The OIG generally agrees with the CIO on the number of information systems used or operated by a contractor of the agency or other organization on behalf of the agency	Yes
The agency inventory is maintained and updated at least annually	Yes
The POA&M is an agency wide process, incorporating all known IT Security weaknesses associated with information systems used or operated by the agency or by a contractor of the agency or other organization on behalf of the agency	Sometimes (51-70% of the time)
OIG Findings are incorporated into the POA&M process	Mostly (81-95% of the time)
Effective POA&M process	Yes
There is an agency wide security configuration policy	Yes
The agency follows documented policies and procedures for identifying and reporting incidents internally	No
The agency follows documented policies and procedures for external reporting to law enforcement authorities	Yes
The agency follows defined procedures for reporting to the USCERT	Yes
The agency has ensured security training and awareness of all employees, including contractors with significant IT security responsibilities	Mostly (81-95% of employees)
The agency explains policies regarding peer-to-peer file sharing in IT security awareness training, ethics training, or any other agency-wide training	Yes
Quality of the agency's PIA process, as discussed in Section D 11.4 (SAOP template), including adherence to existing policy, guidance and standards	Satisfactory
The agency has completed system e-authentication risk assessments	Yes

Department of Treasury -- Privacy Report

Systems that contain Federal information in identifiable form	439	
Agency	428	
Contractor	11	
Systems requiring a Privacy Impact Assessment under the E-Gov Act	348	
Agency	339	
Contractor	9	
Systems covered by an existing Privacy Impact Assessment	330	95%
Agency	321	
Contractor	9	
Systems for which a system or records notice (SORN) is required under the Privacy Act	310	
Agency	302	
Contractor	8	
Systems for which a current SORN has been published in the Federal Register	303	98%
Agency	295	
Contractor	8	
The privacy official participates in all agency information privacy compliance activities	Yes	
The privacy official participates in evaluating the ramifications for privacy of legislative, regulatory and other policy proposals, as well as testimony and comments under Circular A-19	Yes	
The privacy official participates in assessing the impact of technology on the privacy of personal information	Yes	
The agency has a training program to ensure all agency personnel and contractors with access to Federal data are generally familiar with information privacy laws, regulations and policies and understand the ramifications of inappropriate access and disclosure?	Yes	
The agency has a program for job-specific information privacy training for individuals involved in the administration of personal information or information technology systems, or with significant information security responsibilities	Yes	
The agency has written processes or policies for all listed aspects of Privacy Impact Assessments	Yes	
The agency has written process for determining continued compliance with stated web privacy policies	Yes	
Agency uses persistent tracking technology on any web site	Yes	
Agency annually reviews the use of persistent tracking	No	
Agency has current documentation demonstrating review of compliance with information privacy laws, regulations and policies	Yes	
Agency can provide documentation demonstrating corrective action planned, in progress, or completed to remedy identified compliance deficiencies	Yes	
Agency uses technologies that allow for continuous auditing of compliance with stated privacy policies and practices	Yes	
Agency coordinates with OIG on privacy program oversight	Yes	

-This page left blank intentionally-

Department of Veterans Affairs -- CIO Report

Total Number of Systems	602	
Agency Systems	591	
High	306	
Moderate	70	
Low	214	
Not categorized	1	
Contractor Systems	11	
High	3	
Moderate	2	
Low	6	
Not categorized	0	
Certified and Accredited Systems - Total	584	97%
High	307	99%
Moderate	62	86%
Low	215	98%
Not categorized	0	0%
Tested Security Controls - Total	601	100%
High	309	100%
Moderate	72	100%
Low	220	100%
Not categorized	0	0%
Tested Contingency Plans - Total	152	25%
High	94	30%
Moderate	8	11%
Low	50	23%
Not categorized	0	0%
Total # of Systems not Categorized	1	
Incidents Reported to USCERT	2627	
Incidents Reported to Law Enforcement	170	
Total Number of Employees	346,419	
Employees that received IT security awareness training	329,604	95%
Employees that received IT security awareness training using ISSLOB	0	
Total Number of Employees w/significant IT security responsibilities	12,454	
Employees with significant responsibilities that received training	12,454	100%
Total Costs for providing IT security training	$1,312,000	
The agency explains policies regarding peer-to-peer file sharing in training	Yes	
There is an agency-wide security configuration policy	Yes	
The agency applies common security configuration established by NIST to application information systems	Rarely (0-50% of the time)	
The agency has documented in its security policies special procedures for using emerging technologies and countering emerging threats	Yes	

Department of Veterans Affairs -- IG Report

Quality of agency C&A process	Poor
The Agency performs oversight and evaluation to ensure information systems used or operated by a contractor of the agency or other organization on behalf of the agency meet the requirements of FISMA, OMB Policy and NIST guidance	Rarely (0-50% of the time)
The agency has developed an inventory of major information systems, including an identification of interfaces (including those not under control of the agency)	The inventory is approximately 81-95% complete
The OIG generally agrees with the CIO on the number of agency owned systems	Yes
The OIG generally agrees with the CIO on the number of information systems used or operated by a contractor of the agency or other organization on behalf of the agency	No
The agency inventory is maintained and updated at least annually	Yes
The POA&M is an agency wide process, incorporating all known IT Security weaknesses associated with information systems used or operated by the agency or by a contractor of the agency or other organization on behalf of the agency	Sometimes (51-70% of the time)
OIG Findings are incorporated into the POA&M process	Rarely (0-50% of the time)
Effective POA&M process	No
There is an agency wide security configuration policy	Yes
The agency follows documented policies and procedures for identifying and reporting incidents internally	Yes
The agency follows documented policies and procedures for external reporting to law enforcement authorities	Yes
The agency follows defined procedures for reporting to the USCERT	Yes
The agency has ensured security training and awareness of all employees, including contractors with significant IT security responsibilities	Frequently (71-80% of employees)
The agency explains policies regarding peer-to-peer file sharing in IT security awareness training, ethics training, or any other agency-wide training	Yes
Quality of the agency's PIA process, as discussed in Section D 11.4 (SAOP template), including adherence to existing policy, guidance and standards	Poor
The agency has completed system e-authentication risk assessments	Yes

Department of Veteran Affairs -- Privacy Report

Systems that contain Federal information in identifiable form	191	
Agency	191	
Contractor	0	
Systems requiring a Privacy Impact Assessment under the E-Gov Act	186	
Agency	186	
Contractor	0	
Systems covered by an existing Privacy Impact Assessment	181	97%
Agency	181	
Contractor	0	
Systems for which a system or records notice (SORN) is required under the Privacy Act	186	
Agency	186	
Contractor	0	
Systems for which a current SORN has been published in the Federal Register	179	96%
Agency	179	
Contractor	0	
The privacy official participates in all agency information privacy compliance activities	Yes	
The privacy official participates in evaluating the ramifications for privacy of legislative, regulatory and other policy proposals, as well as testimony and comments under Circular A-19	Yes	
The privacy official participates in assessing the impact of technology on the privacy of personal information	Yes	
The agency has a training program to ensure all agency personnel and contractors with access to Federal data are generally familiar with information privacy laws, regulations and policies and understand the ramifications of inappropriate access and disclosure?	Yes	
The agency has a program for job-specific information privacy training for individuals involved in the administration of personal information or information technology systems, or with significant information security responsibilities	Yes	
The agency has written processes or policies for all listed aspects of Privacy Impact Assessments	Yes	
The agency has written process for determining continued compliance with stated web privacy policies	Yes	
Agency uses persistent tracking technology on any web site	No	
Agency annually reviews the use of persistent tracking	Yes	
Agency has current documentation demonstrating review of compliance with information privacy laws, regulations and policies	Yes	
Agency can provide documentation demonstrating corrective action planned, in progress, or completed to remedy identified compliance deficiencies	Yes	
Agency uses technologies that allow for continuous auditing of compliance with stated privacy policies and practices	Yes	
Agency coordinates with OIG on privacy program oversight	Yes	

-This page left blank intentionally-