

## TECHNICAL EXHIBIT 2 Information Assurance

PARAGRAPH NUMBER	TITLE	Narrative Description
<b>C.5.4</b>	<b><i>Information Assurance</i></b>	
<b>C.5.4.1.</b>	<b>Information Assurance (IA) Program Mgmt</b>	
	A Security Program Provided	Number of Security Programs developed, established, managed, and maintained according to regulation
	An IA Law, Policy, or Regulation Change Reviewed.	Number of IA changes including, business processes, procedures and policies
	An IA User-Training Program Provided	All of computer users receive INFOSEC (Information Security) training prior to using the system and are retrained annually
	IA Personnel Trained.	Number of designated IA personnel to be trained
	An IA Appointment Letter Written and Maintained.	Number of appointment letters collected and maintained for all IA personnel
	An IA Memorandum of Agreement/Memorandum of Understanding (MOA/MOU) Maintained.	Number of IA agreements collected and maintained
	A Software License Maintained.	Number of software licenses maintained ensuring that security related documentation is current and accessible to properly authorized individuals.
	An IA Report, Recommendation, or Briefing Completed or Meeting Held.	Total number of reports, recommendations, briefings and meetings at all levels to keep personnel abreast of the latest security threats that are presented to DA, DoD, OMB, or other agencies.
	IA Information Disseminated.	Dissemination of IA communications quarterly or as needed basis - Examples: <ul style="list-style-type: none"> <li>· Publication of IA SOPs on an intranet or via e-mail</li> <li>· Posting of IA staff and contact information</li> <li>· Publication of articles in COE newsletters</li> <li>· IA posters in the corridors and break areas</li> <li>· Summaries of published articles</li> <li>· Product reviews</li> <li>· Lessons learned</li> <li>· Other</li> </ul>

## TECHNICAL EXHIBIT 2 Information Assurance

	An IA Report Prepared	Number of IA reports - Examples: · MFR on an IA topic · Official data call to higher HQ · Letter explaining IA issues to another office
	A Risk Mitigation Recommended	Number of recommendations to mitigate risk through the use of policies and SOPs.
	An IA Inquiry Resolved	Number of inquiries (i.e. email, meetings, discussions, IA related helpdesk tickets)
	IA Threats and Vulnerabilities Evaluated.	Number threats and vulnerabilities studied. For example, include evaluation of situational Awareness Reports (SARs), reading IA publications, web sites, studies, and recommending actions.
	A Security Audit, Inspection or Investigation Conducted	Number of official audits, inspections, and investigations This includes AAA audits, internal reviews, DoDIG inspections, command inspections, fraud, waste and abuse investigations, and other similar activities.
	An audit trail, review, and archive is established and maintained.	Number of devices with audit logs. For example audit trails are established and maintained for servers, routers, switches, RADIUS servers, VPN concentrators, Firewalls, IDSs, and other similar devices.
	An IA Issue Coordinated With Other Agencies.	Number of issues requiring coordination. For example coordination of NETCOM, Army Theater, DoD activities, and agencies on strategic plans and technical guidance translated into objectives, strategies, and architectural guidance
	An IA Issue Coordinated with COE program.	Number of IA coordination issues. For example: CeA Architecture, CPOC/CPAC, Unions
	A Networkiness Certification Completed.	Number of certifications in alignment with NETCOM CONOPS completed
	A Budget is Executed and Managed.	Annual submitted and executed budget (ISSP and MDEPs, MS4X, and MX5T)
	IA Procurements Reviewed.	Number of IA procurements reviewed to ensure they comply with Army architecture and policy guidance
	Participated on Configuration Management Board.	Number of boards where one exists.
	An IA Inspection Conducted	Number of scheduled and unscheduled IA inspections with reports.

## TECHNICAL EXHIBIT 2 Information Assurance

<b>C.5.4.2.</b>	<b><i>Manage userIDs and passwords for all systems. Enforce system access, operation, maintenance and disposition in accordance with policies and practices.</i></b>	
	An Unclassified Account, Password, Permission, Inactivity or Suspension Policy Managed.	Number of unclassified user accounts audited.
	A Classified Account, Password, Permission, Inactivity or Suspension Policy Managed.	Number of classified user accounts audited.
	A New User Created.	Assure that new users agree to appropriate use policies, have proper clearance, have completed INFOSEC training, and have a legitimate "need to know" before issuing userIDs and passwords.
	An IA Personnel Security Clearance Verified.	The number of IA personnel, to include system and/or network administrators, who are designated IT-I, IT-II or IT-III with appropriate security clearance.
	A UserID and Password Disabled.	Number of users who leave the organization. Passwords and userIDs are disabled after the user leaves the organization.
	A default, guest or services accounts removed, changed or disabled.	Number of systems or devices with default, guest or service accounts
	An Privileged Account Issued.	Number of separate accounts issued with increased privileges for SA/NM privileged level and general user access.
	A Password Reissued.	The number of lost, forgotten, or compromised passwords reissued.
	Verification for INFOSEC Training Provided.	The number of verifications of INFOSEC training provided to other organizations - Examples: CPAC requests verification to notify Army that Corps employee has received INFOSEC training.
	A Password Compliance Tested	The number of complexity tests performed to assure strong password compliance per AR-25-2.
	An Illegal Logon Tracked.	Number of log file reviews
	IA Annual Training.	Number Personnel trained and number of courses taught or attended.
<b>C.5.4.3.</b>	<b><i>Certification and Accreditation</i></b>	

## TECHNICAL EXHIBIT 2 Information Assurance

	A DITSCAP Approved. Unclassified	Number of AISs, number of un-classified LANs, number of classified LANs, and the number of SCADA LANs requiring accreditation. Ensure that all ISs within the scope of responsibility are properly certified and accredited in accordance with DITSCAP and configuration management policies and practices before operating or authorizing the use of hardware and software on an IS or network per current AR 25-2.
	A DITSCAP Approved. Classified	Number of AISs, number of un-classified LANs, number of classified LANs, and the number of SCADA LANs requiring accreditation. Ensure that all ISs within the scope of responsibility are properly certified and accredited in accordance with DITSCAP and configuration management policies and practices before operating or authorizing the use of hardware and software on an IS or network per current AR 25-2.
	A Reaccreditation Approved Unclassified	Number of reaccreditations per AR 25-2.
	A Reaccreditation Approved Classified	Number of reaccreditations per AR 25-2.
	An IA Security Tool is Planned and Purchased.	Number of DITSCAP or IA security tools. Serve as functional proponent for DITSCAP software or tools
<b>C.5.4.4.</b>	<b><i>Provide DoD PKI Support</i></b>	
	A DoD PKI Supported	Number of updates to revocation server and number of revocation servers
	A Common Access Card Authentication Supported.	Number of trouble calls for CAC authentication issues - Example: Lost PIN, name change, or lost CAC card.
	A Common Access Card device supported. Work Station	Number Deers Rapid, Mobile Deers Rapid, and CAC Pin Reset devices supported.
	A Common Access Card device supported. Mobil	Number Deers Rapid, Mobile Deers Rapid, and CAC Pin Reset devices supported.
	A Common Access Card device supported. Pin Reset	Number Deers Rapid, Mobile Deers Rapid, and CAC Pin Reset devices supported.
	A CEFMS signature card requested.	The number of CEFMS signature cards requested for initial issuance, or reissuance due to loss or name change.
<b>C.5.4.5.</b>	<b><i>Perform COMSEC</i></b>	
	A COMSEC Inspection Program is Established and Maintained.	The number of COMSEC inspections in accordance with AR 380-53

## TECHNICAL EXHIBIT 2 Information Assurance

	A Sub-Account Reviewed.	Number of sub-accounts and hand receipt holders reviewed to ensure compliance with existing COMSEC material security, accounting, and operational policies/procedures
	A Hand Receipt Holder Reviewed.	Number of sub-accounts and hand receipt holders reviewed to ensure compliance with existing COMSEC material security, accounting, and operational policies/procedures
	A Key Vial, U.S. Flag Carrier or Foreign Commercial Aircraft Transported Outside the Continental U.S. Approved.	Number of key transports outside the continental U.S. approved in accordance with AR380-53
	A Waiver to the Grade Restrictions for COMSEC is Submitted and Approved.	Number of waiver requests
	A Department of Army Cryptographic Access Program is Implemented and Monitored.	Number of DACAP
	A Department of Army Cryptographic Access Program Point of Contact Designated.	Number of DACAP POCs for the INSCOM supporting polygraph element
	A Scheduled Report Provided.	Number of INSCOM reports as specified by AR 380-53
	A COMSEC Inspector, Custodian and Alternate are Appointed.	Number of COMSEC Inspectors, Custodians and Alternates as applicable. In accounts that also contain material controlled under CJCSI 3260.01, assure a custodian and at least four custodian alternates are appointed
	A COMSEC Record is Created and Preserved.	Records are created and preserved as required by AR 380-53
	An Employee is Briefed, Certified or Terminated	Number of personnel who require cryptographic access are briefed, certified or terminated in accordance with AR 380-53
	A Classified Material is Distributed and Maintained	Number of cubic feet of classified COMSEC materials distributed and maintained in support of organizational missions per AR 380-53.
	A Management Control Reviews Performed.	Number of reviews in accordance with AR 380-53
	An Electronic Key Required	Number of keying and re-keying operations for COMSEC equipment
	A Sub-Account Established	Number of sub-accounts in accordance with AR 380-53
	A COMSEC Risk Assessments Conducted.	Number of assessments performed in accordance with AR 380-53
	An Incident Reported	Number of incidents reported including any occurrence, circumstance, or act that could jeopardize the security/integrity of COMSEC material

## TECHNICAL EXHIBIT 2

### Information Assurance

	A COMSEC Employee Trained.	Number of COMSEC personnel trained in accordance with AR 380-53.
	An Incident Resolved	Number of incidents appropriately resolved to include containment, investigation, mitigation and report in accordance with AR 380-53.
<b>C.5.4.6.</b>	<b><i>Information Assurance Vulnerability Alert (IAVA) Reporting and Compliance (24/7 as required) including Bulletins (IAVB), Technical Tips (IAVTT) and Situational Awareness Reports (SARs)</i></b>	
	An IAVA, IAVB, IATT, or SAR notice is coordinated and distributed.	Number of coordinated and distributed IAVA notices sent to identified IA designated employees.
	An IAVA or IAVB is acknowledged.	The number of IAVA and IAVB notices received requiring acknowledgement
	An IAVA notice completed and reported to higher headquarters.	The number of IAVA notices requiring compliance. Required actions are completed on identified affected systems and reported to higher headquarters.
	A required scan performed.	The number of IAVA alerts requiring scans. Run the officially approved scanner to verify compliance with IAVA required actions.
	An IA software patch is applied or a configuration change is made and documented.	Number of IA software patches applied and configuration changes made and documented. Ensure security configurations include all pertinent patches and fixes by routinely reviewing vendor sites, bulletins, and notifications and proactively updating systems with fixes, patches, definitions, and service packs.
	Populate the Compliance Reporting Database (CRD2) and maintain to current IAVA compliance	Number of assets and personnel records entered and maintained in CRD2 for CEEIS.
<b>C.5.4.7.</b>	<b><i>Monitor and Manage Network Security (24/7 as required)</i></b>	
	A network scan completed	The number of enclaves scanned with security scanners including reporting results to the IAM.
	An anomaly reported	Number of anomalies discovered and reported.
	A trend analysis conducted.	The number of trends analyses conducted
	A Security Issue Coordinated	The number of cross-functional coordinations to mitigate or address security issues

## TECHNICAL EXHIBIT 2 Information Assurance

	A Web-page is reviewed for personally identifying (or other inappropriate information) and conformance to the American Disabilities Act (ADA-Section 508 compliance)	Number of times web-pages are reviewed for personally identifying information or ADA conformance. Each individual web-page reviewed would count as one.
	A Official or Local Policy Established	The number of hardware/software security configurations policies established.
	A Firewall system provided.	The number of firewall systems designed, installed, configured, monitored and maintained at each installation.
	An Antivirus Software system upgraded and updated.	Number of hardware devices requiring antivirus software per AR 25-2.
	An IDS System Maintained.	Number of IDS systems designed, installed, configured, monitored and maintained.
	A VPN Concentrator Installed	Number of VPN concentrators designed, installed, configured, monitored and maintained.
	A Physical Restricted Area Policy Enforced.	Number of "restricted areas" in "classified," "unclassified" and "unclassified with limited access" enclaves
	A Physical Restricted Area Policy Enforced.	Number of "restricted areas" in "classified," "unclassified" and "unclassified with limited access" enclaves
	An enclave is established.	The number of enclaves established and maintained networks per AR 25-2
	An enclave is established.	The number of enclaves established and maintained networks per AR 25-2
	A Remote Access Server (RAS) Managed.	Number of remote access servers configured in accordance with regulations and policies.
	A Wireless Access Concentrator Maintained.	Number of wireless access concentrators Designed, installed, configured, monitored, and maintained in accordance with current regulations and policies
	A wireless security review is conducted	Number of times wireless security is reviewed for rogue access points, unauthorized clients, etc.
	An Internet Filtering Software System Maintained.	Number of Internet filtering software systems designed, installed, configured, monitored, and maintained in accordance with AR 25-2 and Army directives

## TECHNICAL EXHIBIT 2

### Information Assurance

	An Intrusion Test Performed.	The number of authorized intrusion tests, war-dialing or other tests successfully performed to assure system integrity and that security policies are in place.
	An Anti-Spam, Spyware and Adware System Maintained. Unclassified	The number of Anti-Spam, Spyware and Adware prevention Systems designed, installed, configured, monitored and maintained.
	An Anti-Spam, Spyware and Adware System Maintained. Classified	The number of Anti-Spam, Spyware and Adware prevention Systems designed, installed, configured, monitored and maintained.
<b>C.5.4.8.</b>	<b><i>Security Incidents</i></b>	
	A Security Incident Reported.	The number of security incidents reported, identified, investigated, mitigated, and contained, and provide recovery for all security incidents per AR 25-2 and current Army policy.
	An Incident Log History Provided.	The number requests for incident investigation log histories.
	A virus is found and removed.	Number of times a virus is found from a computer (PC, Server, PDA, etc.). Each individual device where a virus is found and removed would count as one. Do not include viruses blocked before infection.
	A Device Purged.	The number of devices requiring clearing, purging and releasing memory, media, output devices subsequent to a security incident per AR-25-2 (not including normal disposal of excess equipment – see 4.9.1).
	An IA Incident Processed.	The number of IA incidents processed to include capturing events, conducting after-action reports, providing, implementing, and disseminating lessons learned.
<b>C.5.4.9.</b>	<b><i>Hard Drives excessed</i></b>	
	A Hard Drive Wiped.	The number of hard drives, thumb drive, or other storage media destroyed on excess computers
	A New System Evaluated	The number of new systems (hardware/software) evaluated for security compliance.
<b>C.5.4.10</b>	<b>A System Backup Completed</b>	The number of system backups completed and stored off-site according to AR 25-2 for all systems requiring backup.

**TECHNICAL EXHIBIT 2  
Information Assurance**

PARAGRAPH NUMBER	TITLE	CELRB			CELR C			CELR E			CELR H			CELR L			CELR N			CELR P			CELR D			CELR D TOTALS			
		FY03	FY04	FY05	FY03	FY04	FY05	FY03	FY04	FY05	FY03	FY04	FY05	FY03	FY04	FY05	FY03	FY04	FY05	FY03	FY04	FY05	FY03	FY04	FY05	FY03	FY04	FY05	
<b>C.5.4</b>	<b>INFORMATION ASSURANCE</b>																												
<b>C.5.4.1.</b>	<b>Manage Information Assurance Program</b>																												
	A Security Program Provided	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	8	
	An IA Law, Policy, or Regulation Change Reviewed.	30	30	30	20	20	20	60	60	90	3	13	15	21	30	36	25	35	40	18	20	20	10	10	10	187	218	261	
	An IA User-Training Program Provided	312	304	315	240	231	370	508	401	603	1060	1010	1058	1273	1271	1453	815	786	822	593	670	676	156	152	135	4957	4825	5432	
	IA Personnel Trained.	13	13	13	10	10	10	2	4	4	18	21	24	1243	1272	1275	25	28	29	19	19	18	2	2	2	1332	1369	1375	
	An IA Appointment Letter Written and Maintained.	5	5	5	25	25	25	2	4	4	4	4	4	29	32	30	5	5	5	19	19	18	2	2	2	91	96	93	
	An IA Memorandum of Agreement/Memorandum of Understanding (MOA/MOU) Maintained.	2	2	2	3	3	6	20	30	40	3	7	8	0	4	4	33	33	33	0	2	9	1	1	100	62	82	202	
Workload data in TE 2 GFE	A Software License Maintained.																												
	An IA Report, Recommendation, or Briefing Completed or Meeting Held.	75	150	150	25	25	25	24	24	36	55	73	83	55	55	60	18	42	42	52	75	100	50	50	50	354	494	546	
	IA Information Disseminated.	40	100	120	150	150	150	180	180	190	223	164	180	30	33	33	14	16	16	540	690	700	55	55	55	1232	1388	1444	
	An IA Report Prepared	35	65	65	80	100	120	5	5	10	45	60	69	45	58	60	35	40	40	5	8	10	50	50	50	300	386	424	
	A Risk Mitigation Recommended	7	8	10	5	5	6	10	10	10	2	5	10	11	14	16	3	3	2	2	2	25	25	25	65	72	82		
	An IA Inquiry Resolved	2000	4200	4200	300	300	300	500	500	500	450	726	850	2500	2500	2500	400	470	520	156	156	156	100	100	100	6406	8952	9126	
	IA Threats and Vulnerabilities Evaluated.	100	150	200	150	150	150	70	150	300	245	180	198	200	200	200	25	40	40	52	52	52	90	90	90	932	1012	1230	
	A Security Audit, Inspection or Investigation Conducted	8	8	8	5	5	5	4	4	8	15	17	19	8	9	10	3	3	3	19	19	20	4	4	4	66	69	77	
Workload data in TE 2 GFE	An audit trail, review, and archive is established and maintained.																												
	An IA Issue Coordinated With Other Agencies.	4	4	6				3	3	3	2	3	3	5	15	15										14	25	27	
	An IA Issue Coordinated with COE program.	32	36	40	12	12	12	10	10	15	24	36	36	11	13	12	6	6	6	8	8	11	2	3	3	105	124	135	
	A Network Certification Completed.	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	2	
	A Budget is Executed and Managed.	2	2	2	2	2	2	2	2	2	2	2	2	1	1	1	6	9	7	1	1	1	2	2	2	18	21	19	
	IA Procurements Reviewed.	1	1	1	1	1	1	1	1	1	5	10	12	0	1	6	1	1	1	3	3	4	1	1	1	13	19	27	
	Participated on Configuration Management Board.	0	0	0	1	1	1	1	1	1	1	1	1	0	0	1	1	1	1	0	0	1	1	1	1	5	5	7	
	An IA Inspection Conducted	48	48	48	12	12	12	52	52	52	168	336	336	0	0	0	240	240	240	0	0	0	14	28	28	534	716	716	
<b>C.5.4.2.</b>	<b>Manage userIDs and passwords for all systems. Enforce system access, operation, maintenance and disposition in accordance with policies and practices.</b>																												
Workload data in TE 2 C.5.2.7.1	An Unclassified Account, Password, Permission, Inactivity or Suspension Policy Managed.																												
Workload data in TE 2 C.5.2.7.2	A Classified Account, Password, Permission, Inactivity or Suspension Policy Managed.																												
	An IA Personnel Security Clearance Verified	5	15	15	10	10	10	20	20	20	60	72	72	0	1	1	4	8	8	19	19	19	0	0	0	118	145	145	
	A default, guest or services accounts removed, changed or disabled.	120	135	150	80	80	80	150	125	130	146	161	176	400	400	400	212	212	215	775	557	557	35	35	35	1918	1705	1743	
	An Privileged Account Issued.	8	8	8	30	30	30	5	7	10	59	69	73	146	146	146	12	12	12	720	720	557	8	8	8	988	1000	844	
	A Password Reissued.	48	48	48	10	10	50	20	20	20	24	26	26	12	12	24	79	91	88	154	286	250	2	3	3	349	496	509	
	Verification for INFOSEC Training Provided.	10	10	12	5	5	5	0	10	10	17	20	22	2	2	2	0	0	0	19	19	19	0	0	0	53	66	70	
	A Password Compliance Tested	48	48	48	0	1	2	24	24	24	2	4	4	0	4	4	4	4	0	0	0	2	2	2	2	80	87	88	
	An Illegal Logon Tracked.	240	240	240	250	250	250	365	365	365	0	0	0	420	480	600	52	53	52	0	0	0	50	400	300	1377	1788	1807	
	IA Annual Training.																												
<b>C.5.4.3.</b>	<b>Certification and Accreditation</b>																												
	A DITSCAP Approved. Unclass	1	1	1	0	0	1	1	1	1	1	0	1	0	0	1	1	1	1	1	1	1	0	1	1	5	5	8	
	A DITSCAP Approved. Class	0	0	0	0	0	1	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	1	1	0	2	2	
	A Reaccreditation Approved Unclass	1	1	1	0	0	1	1	1	1	0	1	2	0	0	1	0	0	1	0	0	1	1	1	1	3	4	9	
	A Reaccreditation Approved Class	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0	1	1	1	0	2
	An IA Security Tool is Planned and Purchased.	0	0	2	0	1	2	1	3	2	3	5	7	0	1	1				3	3	5	2	2	2	9	15	21	
<b>C.5.4.4.</b>	<b>Provide DoD PKI Support</b>																												
	A DoD PKI Supported	0	0	0	0	0	0																						
	A Common Access Card Authentication Supported.	0	0	120	0	5	100	0	0	0	2	4	900	0	76	136	0	13	1010	0	0	100	0	7	125	2	105	2491	
	A Common Access Card device supported. Work Sta	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	
	A Common Access Card device supported. Mobile	0	0	0	0	1	1	0	0	0	0	1	1	0	1	1	0	1	1	0	0	0	0	0	0	0	4	4	
	A Common Access Card device supported. Pin Rese	0	0	1	0	0	0	0	0	0	0	5	5	0	0	2	0	1	1	0	0	1	0	0	1	0	6	11	
	A CEFMS signature card requested.	75	90	110	50	50	50	114	114	114	347	122	175	498	232	191	114	100	107	272	60	60	30	30	25	1500	798	832	
<b>C.5.4.5.</b>	<b>Perform COMSEC</b>																												
	A COMSEC Inspection Program is Established and Maintained.	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3	3	3	0	0	0	0	0	0	3	3	3	



**TECHNICAL EXHIBIT 2  
Information Assurance**

	An Anti-Spam, Spyware and Adware System Maintained. Unclassified	280	300	350	0	215	215	0	0	1	1051	1046	2064	40	60	1200	0	70	100	0	0	1	10	10	10	1381	1701	3941	
	An Anti-Spam, Spyware and Adware System Maintained. Classified																												
<b>C.5.4.8.</b>	<b>Security Incidents</b>																												
	A Security Incident Reported.	0	0	0	1	0	0	0	0	0	0	0	0	1	0	0	0	0	0	1	0	0	3	0	0				
	An Incident Log History Provided.	0	2	0	0	20	5	1	2	3	3	6	5	6	6	6	12	12	12	4	5	5	0	0	0	26	53	36	
	A virus is found and removed.	0	5	10	2	1	5	30	25	20	17	21	25	62	20	22	8	8	8				1	1	1	120	81	91	
	A Device Purged.	0	6	3	2	2	3	25	25	25	24	36	36	6	6	6	12	12	12	3	1	2	0	0	0	72	88	87	
	An IA Incident Processed.	0	1	1	0	1	1	0	1	2	5	8	8	1	6	0	0	0	0	4	3	2	6	6	6	16	26	20	
<b>C.5.4.9.</b>	<b>SA / IASO responsibilities</b>																												
	A Hard Drive Wiped.	84	84	84	40	50	50	125	100	100	180	240	240	433	220	280	259	174	216.5	50	50	75	35	35	35	1206	953	1080.5	
	A New System Evaluated	96	96	96	2	2	5	140	140	140	180	240	240	35	28	20	150	150	120	258	200	187	6	6	6	867	862	814	
<b>C.5.4.10.</b>	<b>A System Backup Completed</b>	800	830	850	468	468	936	9053	9053	9053	17395	22860	387860	8160	8400	8400	4800	4800	8400	240	240	240	2600	2600	2600	43516	49251	418339	

**TECHNICAL EXHIBIT 2  
Information Assurance**

PARAGRAPH NUMBER	TITLE	CEMVK			CEMVM			CEMVN			CEMVP			CEMVR			CEMVS			CEMVD			CEMVD TOTALS		
		FY03	FY04	FY05	FY03	FY04	FY05	FY03	FY04	FY05	FY03	FY04	FY05	FY03	FY04	FY05	FY03	FY04	FY05	FY03	FY04	FY05	FY03	FY04	FY05
<b>C.5.4</b>	<b>INFORMATION ASSURANCE</b>																								
<b>C.5.4.1</b>	<b>Manage Information Assurance Program</b>																								
	A Security Program Provided	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	9	9	9
	An IA Law, Policy, or Regulation Change Reviewed.	0	0	0	8	8	8	34	36	36	7	8	8	2	4	6	12	12	12	1	4	3	64	72	73
	An IA User-Training Program Provided	1340	1216	1479	664	631	679	1594	1403	1625	758	731	777	942	929	1080	819	726	860	224	136	183	9021	8730	9641
	IA Personnel Trained.	25	56	56	6	9	15	31	31	31				6	6	6	18	18	18	0	7	9	136	239	247
	An IA Appointment Letter Written and Maintained.	2	3	3	6	9	15	30	30	30	6	5	5	6	6	6	15	15	15	2	2	2	71	76	82
	An IA Memorandum of Agreement/Memorandum of Understanding (MOA/MOU) Maintained.	4	14	13	2	4	4	3	3	5	3	3	4	0	1	1	4	4	4	3	7	7	27	62	64
Workload data in TE 2 GFE	A Software License Maintained.																								
	An IA Report, Recommendation, or Briefing Completed or Meeting Held.	107	155	170	24	24	24	80	100	120	22	15	15	4	12	12	165	217	269	57	57	57	673	920	1007
	IA Information Disseminated.	52	52	52	112	112	60	48	44	48	48	60	60	50	50		85	150	215	52	52	52	551	624	591
	An IA Report Prepared	150	200	220	60	60	60	120	120	120	5	6	6	30	50	100	49	68	87	0	0	0	714	944	1033
	A Risk Mitigation Recommended	1	2	2	220	220	220	1	8	5	5	6	6	0	1	2	10	5	8	1	2	2	240	248	249
	An IA Inquiry Resolved	175	200	250	49	31	35	4542	4600	4700	173	210	210	12	15	18	920	824	680	44	50	63	6265	6430	6456
	IA Threats and Vulnerabilities Evaluated.	150	200	220	100	100	100	380	392	420	12	15	15	3	5	12	35	66	97	150	200	220	1130	1418	1524
	A Security Audit, Inspection or Investigation Conducted	1	2	1	1	3	1	2	2	2	1	1	1	1	1	1	2	2	2	1	1	1	11	14	11
Workload data in TE 2 GFE	An audit trail, review, and archive is established and maintained.																								
	An IA Issue Coordinated With Other Agencies.	2	2	2	12	12	12	12	12	12	0	0	0	0	1	1	3	2	2	1	1	1	34	34	34
	An IA Issue Coordinated with COE program.	12	12	12	84	84	84	24	24	24	2	36	36	2	4	4	56	80	104	6	6	6	210	270	294
	A Networkiness Certification Completed.	0	0	0	0	0	0	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1
	A Budget is Executed and Managed.	3	3	3	2	2	2	2	2	2	1	1	1	3	3	3	2	2	2	3	3	3	22	22	22
	IA Procurements Reviewed.	1	1	1	0	0	2	1	1	1	10	12	12	1	1	1	7	7	9	1	1	1	23	25	29
	Participated on Configuration Management Board.	2	2	3	1	2	3	1	2	3	1	1	1	1	2	2	1	2	2	0	0	6	11	17	26
	An IA Inspection Conducted	0	0	6	24	24	24	400	700	1200	96	120	120	24	24	24	6	6	6	0	0	6	550	886	1398
<b>C.5.4.2.</b>	<b>Manage userIDs and passwords for all systems. Enforce system access, operation, maintenance and disposition in accordance with policies and practices.</b>																								
Workload data in TE 2 C.5.2.7.1	An Unclassified Account, Password, Permission, Inactivity or Suspension Policy Managed.																								
Workload data in TE 2 C.5.2.7.2	A Classified Account, Password, Permission, Inactivity or Suspension Policy Managed.																								
	An IA Personnel Security Clearance Verified.	15	20	20	6	9	15	0	0	0	6	6	6	8	8	8	3	3	3	2	2	2	70	88	94
	A default, guest or services accounts removed, changed or disabled.	1,500	1,500	1,500	249	260	296	1,600	1,800	2,000	400	400	400	50	300	300	301	300	302	83	83	83	7183	7643	7881
	An Privileged Account Issued.	17	18	18	35	35	30	30	30	30	15	25	25	12	8	8	37	34	39	17	18	18	197	204	204
	A Password Reissued.	300	336	300	18	92	36	180	277	180	240	600	600	36	36	36	24	25	25	75	95	60	1473	2061	1837
	Verification for INFOSEC Training Provided.	0	1	1	6	6	6	2	2	2	12	24	24	0	0	0	12	12	12	0	1	1	32	48	48
	A Password Compliance Tested	12	12	12	12	12	12	8	12	12	12	12	12	0	0	0	1464	2928	2928	12	12	12	1544	3012	3012
	An Illegal Logon Tracked.	3	2	3	5	3	5	2	2	2	144	144	144	0	0	12	0	4	4	3	3	3	163	164	179
	IA Annual Training.																								
<b>C.5.4.3.</b>	<b>Certification and Accreditation</b>																								
	A DITSCAP Approved. Unclass	2	3	1	1	1	1	1	1	1	2	2	2	0	1	1	0	1	2	2	2	1	12	13	11
	A DITSCAP Approved. Class	0	1	1	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	1	1	0	5	5
	A Reaccreditation Approved Unclass	0	0	0	0	0	1	0	0	1	1	1	1	0	0	0	0	0	0	0	0	0	1	1	4
	A Reaccreditation Approved Class	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	1
	An IA Security Tool is Planned and Purchased.	3	4	1	0	0	2	1	1	1	4	6	6	0	0	0	4	6	8	1	3	1	19	22	21
<b>C.5.4.4.</b>	<b>Provide DoD PKI Support</b>																								
	A DoD PKI Supported	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

**TECHNICAL EXHIBIT 2  
Information Assurance**

	A Common Access Card Authentication Supported.	5	5	60	0	6	12	0	175	200	36	24	24	0	18	300	0	20	200	5	5	60	56	373	976
	A Common Access Card device supported. Work Station	1	1	1	0	1	1	0	1	1	1	1	1	0	0	0	0	0	0	0	0	0	4	6	6
	A Common Access Card device supported. Mobile	1	1	0	0	0	0	0	0	0	1	1	1	0	1	1	0	0	0	0	0	0	4	3	2
	A Common Access Card device supported. Pin Reset	0	0	0	0	0	0	0	0	0	1	1	1	0	0	0	1	1	1	0	0	0	2	2	2
	A CEFMS signature card requested.	214	86	165	147	81	120	314	230	255	30	30	30	20	20	20	48	48	48	72	86	55	1273	911	1023
<b>C.5.4.5.</b>	<b>Perform COMSEC</b>																								
	A COMSEC Inspection Program is Established and Maintained.	0	2	2	0	0	0	1	2	2	1	1	1	0	0	0	1	1	1	0	0	0	3	10	10
	A Sub-Account or Hand Receipt Holder Reviewed. - Sub Account	0	0	0	0	0	0	0	0	0	10	12	12	0	0	0	0	0	0	0	0	0	10	12	12
	A Sub-Account or Hand Receipt Holder Reviewed. - Hand Receipt	6	6	6				12	12	12	10	12	12	0	0	0	0	0	0				40	42	42
	A Key Vial, U.S. Flag Carrier or Foreign Commercial Aircraft Transported Outside the Continental U.S. Approved.	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	A Waiver to the Grade Restrictions for COMSEC is Submitted and Approved.	0	0	0	0	0	0	0	0	0	1	1	1	0	0	0	0	0	0	0	0	0	1	1	1
	A Department of Army Cryptographic Access Program is Implemented and Monitored.	24	24	46	0	0	60	60	60	12	12	12				0	0					0	144	188	210
	A Department of Army Cryptographic Access Program Point of Contact Designated.	12	12	12	0	0	0	0	0	0	12	1	12	0	0	0	0	0	0	0	0	0	48	37	48
	A Scheduled Report Provided.	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	A COMSEC Inspector, Custodian and Alternate are Appointed.	1	1	1	0	0	0	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	4	4	4
	A COMSEC Record is Created and Preserved.	360	360	420	0	0	0	12	12	12	12	12	12	0	0	0	0	0	0	0	0	0	1104	1224	1284
	An Employee is Briefed, Certified or Terminated	1	1	1	0	0	0	0	0	0	24	24	24	0	0	0	1	1	1	1	1	1	29	29	29
	A Classified Material is Distributed and Maintained	1	1	1	0	0	0	12	12	12	144			15	0	0	1	1	1	1	1	1	161	17	32
	A Management Control Reviews Performed.	0	0	1	0	0	0	1	2	2	4	6	6	0	0	0	1	1	1	1	0	0	6	11	13
	An Electronic Key Required	61	63	75	0	0	0	7	5	5	2	2	2	0	0	0	13	13	13	48	48	48	253	281	293
	A Sub-Account Established	0	0	0	0	0	0	0	0	0	12	12	12	0	0	0	0	0	0	0	0	0	12	12	12
	A COMSEC Risk Assessments Conducted.	0	0	0	0	0	0	0	0	0	2	2	2	0	0	0	0	0	0	0	0	1	2	2	3
	An Incident Reported	1	0	0	0	0	0	0	0	0	3	3	3	0	0	0	0	0	0	0	0	0	6	3	3
	A COMSEC Employee Trained.	2	3	4	0	0	0	1	1	1	12	12	12	0	0	0	0	0	2	0	0	0	19	26	25
	An Incident Resolved	1	0	0	0	0	0	0	0	0	6	6	6	0	0	0	0	0	0	0	0	9	6	6	
<b>C.5.4.6.</b>	<b>Information Assurance Vulnerability Alert (IAVA) Reporting and Compliance (24/7 as required) including Bulletins (IAVB), Technical Tips (IAVTT) and Situational Awareness Reports (SARs)</b>																								
	An IAVA, IAVB, IATT, or SAR notice is coordinated and distributed.	51	82	56	51	82	56	51	82	56	51	82	56	51	82	56	51	82	56	51	82	56	459	686	504
	An IAVA or IAVB is acknowledged.	28	54	72	28	54	72	28	54	72	28	54	72	28	54	72	28	54	72	28	54	72	252	522	648
	An IAVA notice completed and reported to higher headquarters.	21	34	48	21	34	48	21	34	48	21	34	48	21	34	48	21	34	48	21	34	48	189	334	432
	A required scan performed.	46	68	96	46	68	96	46	68	96	100	200	250	46	68	96	46	68	96	46	68	96	468	800	1018
	An IA software patch is applied or a configuration change is made and documented.	8575	28175	18375	21600	24000	24000	720000	840000	840000	44	34	36	150	480	500	32,860	45,590	58,320	1288	4228	2758	801667	979257	980739
	Populate the Compliance Reporting Database (CRD2) and maintain to current IAVA compliance																						0	0	0
<b>C.5.4.7.</b>	<b>Monitor and Manage Network Security (24/7 as required)</b>																								
	A network scan completed	48	48	48	240	240	240	96	96	96	96	96	96	24	24	24	147	204	261	48	48	48	795	852	909
	An anomaly reported	144	144	144	180	180	180	1400	1600	1600	96	96	96	3	4	6	247	233	233	48	48	48	2406	2593	2595
	A trend analysis conducted.	0	0	12	0	0	0	0	0	0	12	12	12	0	0	0	2	3	3	0	0	12	14	39	63
	A Security Issue Coordinated	74	100	100	60	60	60	36	48	60	60	72	60	0	0	0	111	134	153	8	10	10	497	624	643
	A Web-page is reviewed for personally identifying (or other inappropriate information)	55780	57500	60240	8864	10429	11993	10753	11291	2258	29700	1500	1500	11300	13118	14400	11300	13118	14400				239257	227436	225271



**TECHNICAL EXHIBIT 2  
Information Assurance**

PARAGRAPH NUMBER	TITLE	CENAB			CENAE			CENAN			CENAO			CENAP			CENAD			CENAD TOTALS			
		FY03	FY04	FY05	FY03	FY04	FY05	FY03	FY04	FY05	FY03	FY04	FY05	FY03	FY04	FY05	FY03	FY04	FY05	FY03	FY04	FY05	
<b>C.5.4</b>	<b>INFORMATION ASSURANCE</b>																						
<b>C.5.4.1</b>	<b>Manage Information Assurance Program</b>																						
	A Security Program Provided	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	6	6	6	
	An IA Law, Policy, or Regulation Change Reviewed.	15	30	29		4	5	1	3	1	26	42	50	1	1	1	1	2	2	44	82	88	
	An IA User-Training Program Provided	1142	1132	1323	617	648	747	762	719	766	633	499	584	509	537	597	147	123	157	3810	3658	4174	
	IA Personnel Trained.	73	65	68	2	2	2	6	6	6	14	6	10	9	9	9	2	3	3	106	91	98	
	An IA Appointment Letter Written and Maintained.	51	52	51	1	1	1	6	6	6	13	8	10	10	10	10	2	3	3	83	80	81	
	An IA Memorandum of Agreement/Memorandum of Understanding (MOA/MOU) Maintained.	11	18	19	2	1	1	2	2	3	3	4	5	4	1	1	1	2	2	23	28	31	
Workload data in TE 2 GFE	A Software License Maintained.																						
	An IA Report, Recommendation, or Briefing Completed or Meeting Held.	48	87	102	70	70	70	48	48	48	160	120	200	20	24	24	10	20	24	356	369	468	
	IA Information Disseminated.	258	274	304	48	48	48	16	16	16	55	95	75	4	8	12	12	15	15	393	456	470	
	An IA Report Prepared	57	68	65	5	5	10	8	8	8	35	42	50	28	37	30	10	12	12	143	172	175	
	A Risk Mitigation Recommended	28	30	31	6	6	6	4	4	4	55	28	30	6	6	6		3	6	99	77	83	
	An IA Inquiry Resolved	1,513	2,101	2,628	20	20	20	6	3	3	175	205	150	24	32	32		20	40	1738	2381	2873	
	IA Threats and Vulnerabilities Evaluated.	1351	1566	1787	100	100	100	42	71	100	40	55	50	36	36	36		30	60	1569	1858	2133	
	A Security Audit, Inspection or Investigation Conducted	4	6	6	3	3	3	5	3	2	3	2	5	1	1	1		6	16	15	23		
Workload data in TE 2 GFE	An audit trail, review, and archive is established and maintained.																						
	An IA Issue Coordinated With Other Agencies.	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
	An IA Issue Coordinated with COE program.	8	28	11	4	4	4	12	12	24	10	5	10	36	60	60	12	17	24	82	126	133	
	A Networkness Certification Completed.	9	10	11	2	2	2	1	1	1	1	1	1	1	1	1	1	1	1	15	16	17	
	A Budget is Executed and Managed.	5	5	5	1	1	1	1	0	1	1	2	1	0	0	0	1	1	1	9	9	8	
	IA Procurements Reviewed.	28	20	21	5	5	5	2	2	2	1	1	1	1	1	1	1	1	1	38	30	31	
	Participated on Configuration Management Board.	1	1	2	1	1	1	1	1	1	0	0	1	0	0	0	1	1	1	4	4	6	
	An IA Inspection Conducted	52	65	72	1	1	1	2	1	1	2	2	2	2	8	6		12	12	16	71	89	98
<b>C.5.4.2.</b>	<b>Manage userIDs and passwords for all systems. Enforce system access, operation, maintenance and disposition in accordance with policies and practices.</b>																						
Workload data in TE 2 C.5.2.7.1	An Unclassified Account, Password, Permission, Inactivity or Suspension Policy Managed.																						
Workload data in TE 2 C.5.2.7.2	A Classified Account, Password, Permission, Inactivity or Suspension Policy Managed.																						
	An IA Personnel Security Clearance Verified.	14	21	25	4	4	0	6	6	6	12	14	3	0	0	0	0	48	72	36	93	106	
	A default, guest or services accounts removed, changed or disabled.	510	539	525	700	611	650	15	15	18	460	443	460	16	20	16	100	125	150	1801	1753	1819	
	An Privileged Account Issued.	36	19	19	5	5	5	12	2	4	2	2	2	6	8	8	1	2	2	62	38	40	
	A Password Reissued.	410	380	262	18	14	15	189	248	260	9	11	26	46	46	24				672	699	587	
	Verification for INFOSEC Training Provided.	106	112	112	5	194	24	12	12	12	4	6	4	0	0	0	0	0	0	127	324	152	
	A Password Compliance Tested	51	52	52	2	2	3	0	0	12	4	3	4	0	0	0	12	12	12	69	69	83	
	An Illegal Logon Tracked.	180	182	180	24	18	23	336	336	336	36	36	100	24	24	24	0	0	0	600	596	663	
	IA Annual Training.																			0	0	0	
<b>C.5.4.3.</b>	<b>Certification and Accreditation</b>																						
	A DITSCAP Approved. Unclass	4	2	5	1	1	1	1	1	1	3	2	1	0	1	0	0	2	1	9	9	9	
	A DITSCAP Approved. Class	1	1	0	1	1	1	1	1	1	0	0	1	0	0	0	0	1	0	3	4	3	
	A Reaccreditation Approved Unclass	3	3	7	0	0	1	0	0	1	0	0	2	0	0	0	0	0	1	3	3	12	
	A Reaccreditation Approved Class	0	0	2	0	0	1	0	0	1	0	0	0	0	0	0	0	0	1	0	0	5	
	An IA Security Tool is Planned and Purchased.	4	5	5	2	2	2	3	4	5	5	2	5	1	1	1	0	2	2	15	16	20	
<b>C.5.4.4.</b>	<b>Provide DoD PKI Support</b>																						

**TECHNICAL EXHIBIT 2  
Information Assurance**

	A DoD PKI Supported	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	10	0	1	10
	A Common Access Card Authentication Supported.	0	3	0	0	0	200	95	164	110	0	0	200	31	76	84	12	12	12	138	255	606	
	A Common Access Card device supported. Work Sta	0	0	0	0	0	0	0	1	1	0	0	0	1	1	0	0	0	0	1	2	1	
	A Common Access Card device supported. Mobile	0	1	0	0	0	0	1	0	0	0	0	0	1	1	0	0	0	1	2	1		
	A Common Access Card device supported. Pin Rese	0	0	0	1	1	1	0	1	1	0	1	1	0	0	0	0	0	1	3	3		
	A CEFMS signature card requested.	328	664	413	80	270	80	127	231	135	62	110	100	197	200	50	10	15	15	804	1490	793	
<b>C.5.4.5.</b>	<b>Perform COMSEC</b>																						
	A COMSEC Inspection Program is Established and Maintained.	2	3	3	0	0	0	1	1	1	0	0	1	2	3	3	0	0	0	5	7	8	
	A Sub-Account or Hand Receipt Holder Reviewed. - Sub Account	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	1	
	A Sub-Account or Hand Receipt Holder Reviewed. - Hand Receipt	15	17	17				12	12	12	2	2	2	0	0	0	0	0	1	29	31	32	
	A Key Vial, U.S. Flag Carrier or Foreign Commercial Aircraft Transported Outside the Continental U.S. Approved.	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	4	0	0	5	
	A Waiver to the Grade Restrictions for COMSEC is Submitted and Approved.	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	0	0	2	
	A Department of Army Cryptographic Access Program is Implemented and Monitored.		0	0		0	0	0	0	0		0	0	0	0	0	0	0	1	0	0	1	
	A Department of Army Cryptographic Access Program Point of Contact Designated.	0	0	0	0	0	0	0	0	0	3	1	0	0	0	0	0	0	2	3	1	2	
	A Scheduled Report Provided.	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	1	0	
	A COMSEC Inspector, Custodian and Alternate are Appointed.	1	1	1	0	0	0	1	1	1	0	0	0	1	1	1	0	0	0	3	3	3	
	A COMSEC Record is Created and Preserved.	12	12	12	0	0	0	24	24	24	2	2	2	12	12	12	0	0	12	50	50	62	
	An Employee is Briefed, Certified or Terminated	24	24	24	0	0	0	0	0	0	2	1	2	24	24	24	0	0	6	50	49	56	
	A Classified Material is Distributed and Maintained	48	48	48	0	0	0	1	1	1	2	2	2	36	36	36	0	0	3	87	87	90	
	A Management Control Reviews Performed.	12	12	12	0	0	0	1	1	1	0	0	1	29	44	40	0	0	1	42	57	55	
	An Electronic Key Required	0	0	0	0	0	0	5	5	5	1	2	1	6	7	8	0	0	4	12	14	18	
	A Sub-Account Established	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	1	
	A COMSEC Risk Assessments Conducted.	0	0	0	0	0	0	1	0	0	12	12	12	6	5	4	0	0	1	19	17	17	
	An Incident Reported	0	0	0	0	0	0	3	0	0	0	0	1	0	0	0	0	0	0	3	0	1	
	A COMSEC Employee Trained.	0	0	0	0	4	0	2	0	2	1	1	1	2	2	2	0	0	2	5	7	7	
	An Incident Resolved	0	0	0	0	0	0	3	0	0	0	0	0	0	0	0	0	0	0	3	0	0	
<b>C.5.4.6.</b>	<b>Information Assurance Vulnerability Alert (IAVA) Reporting and Compliance (24/7 as required) including Bulletins (IAVB), Technical Tips (IAVTT) and Situational Awareness Reports (SARs)</b>																						
	An IAVA, IAVB, IATT, or SAR notice is coordinated and distributed.	51	82	56	51	82	56	51	82	56	51	82	56	51	82	56	51	82	56	306	492	336	
	An IAVA or IAVB is acknowledged.	28	54	72	28	54	72	28	54	72	28	54	72	28	54	72	28	54	72	168	324	432	
	An IAVA notice completed and reported to higher headquarters.	21	34	48	21	34	48	21	34	48	21	34	48	21	34	48	21	34	48	126	204	288	
	A required scan performed.	46	68	96	46	68	96	46	68	96	46	68	96	46	68	96	46	68	96	276	408	576	
	An IA software patch is applied or a configuration change is made and documented.	34258	44001	52127	14,375	30,650	39,000	9510	8504	9434	16200	10500	20000	11200	26320	26880	1000	1500	2000	86543	121475	149441	
	Populate the Compliance Reporting Database (CRD2) and maintain to current IAVA compliance																0	115	50	0	115	50	
<b>C.5.4.7.</b>	<b>Monitor and Manage Network Security (24/7 as required)</b>																						
	A network scan completed	358	436	468	25	50	60	48	48	48	19	65	125	47	101	96	24	48	72	521	748	869	
	An anomaly reported	99	115	129	0	0	0	2	3	0	55	42	80	24	24	24	1	22	24	181	206	257	
	A trend analysis conducted.	56	67	76	0	0	0	0	1	1	25	15	30	0	0	0	0	0	12	81	83	119	
	A Security Issue Coordinated	246	292	344	0	1	2	2	5	0	5	2	10	24	24	24	12	24	34	289	348	414	

**TECHNICAL EXHIBIT 2  
Information Assurance**

	A Web-page is reviewed for personally identifying (or other inappropriate information)				250	400	1205								960	1200	1440	600	783	900	1810	2383	3545
	A Web-page is reviewed for conformance to the American Disabilities Act (ADA-Section 508 compliance)				250	400	1205								960	1200	1440	600	783	900	1810	2383	3545
	A Official or Local Policy Established	195	241	258	1950	2406	2415	5	4	4	110	25	28	2	2	2	96	108	96	2358	2786	2803	
	A Firewall system provided.	3	6	9	1	2	2	0	3	1	2	1	1	2	2	6	0	24	24	8	38	43	
Workload data in TE 2 GFE	An Antivirus Software system upgraded and updated.																						
	An IDS System Maintained.	0	1	1	1	1	2	0	0	0	2	1	0	0	0	0	0	0	0	0	3	3	3
	A VPN Concentrator Installed	0	0	0	1	2	3	0	0	0	0	0	1	0	0	0	0	0	0	1	2	4	
	A Physical Restricted Area Policy Enforced.	432	425	422	6	6	6	1	1	1	1	1	1	1	1	1	0	1	1	441	435	432	
	A Physical Restricted Area Policy Enforced.	13	13	13	1	1	1	1	1	1	2	2	2	1	1	1	0	2	2	18	20	20	
	An enclave is established.	24	24	24	45	45	46	1	1	1	1	1	1	5	5	5	0	16	24	76	92	101	
	An enclave is established.	13	13	23	1	1	1	1	1	1	1	1	1	1	1	1	0	12	12	17	29	39	
	A Remote Access Server (RAS) Managed.	4	6	3	1	2	2	12	12	12	3	1	1	1	1	1	0	12	12	21	34	31	
	A Wireless Access Concentrator Maintained.	0	0	0	0	0	5	0	0	0	0	0	0	0	0	4	0	0	12	0	0	21	
	A wireless security review is conducted				0	0	0							0	0	4	0	1	4	0	1	8	
	An Internet Filtering Software System Maintained.	2	12	13	1	1	2	0	0	0	0	0	0	1	1	1	0	0	12	4	14	28	
	An Intrusion Test Performed.	0	0	0	2	0	2	1	2	1	37	1	20	0	0	0	0	1	1	40	4	24	
	An Anti-Spam, Spyware and Adware System Maintained. Unclassified	57	281	648	0	100	50	0	0	0	0	150	400	0	40	560	0	30	1200	57	601	2858	
	An Anti-Spam, Spyware and Adware System Maintained. Classified																			0	0	0	
<b>C.5.4.8.</b>	<b>Security Incidents</b>																						
	A Security Incident Reported.	3	0	0	1	0	0	0	0	0	2	1	0	0	0	0	0	0	0	6	1	0	
	An Incident Log History Provided.	14	26	37	0	0	0	0	0	0	5	0	1	0	0	0	0	0	0	19	26	38	
	A virus is found and removed.				50	0	0							7	10	15	0	10	15	57	20	30	
	A Device Purged.	16	11	27	150	150	150	8	10	10	10	6	15	0	0	0	30	60	184	207	262		
	An IA Incident Processed.	34	34	36	3	0	3	2	5	0	2	1	1	1	0	0	0	2	1	42	42	41	
<b>C.5.4.9.</b>	<b>SA / IASO responsibilities</b>																						
	A Hard Drive Wiped.	328	407	378	59	32	30	162	117	140	205	109	190	80	150	120	48	60	72	882	875	930	
	A New System Evaluated	706	801	806	121	149	130	74	114	139	210	99	150	80	150	120	0	12	46	1191	1325	1391	
<b>C.5.4.10.</b>	<b>A System Backup Completed</b>	4351	5287	5876	3120	4420	6500	12	32	36	2710	3364	4896	2600	1025	260	96	960	1200	12889	15088	18768	

**TECHNICAL EXHIBIT 2  
Information Assurance**

PARAGRAPH NUMBER	TITLE	CENWK			CENWO			CENWP			CENWS			CENWW			CENWD			CENWD TOTALS		
		FY03	FY04	FY05	FY03	FY04	FY05															
<b>C.5.4</b>	<b>INFORMATION ASSURANCE</b>																					
<b>C.5.4.1</b>	<b>Manage Information Assurance Program</b>																					
	A Security Program Provided	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	6	6	6
	An IA Law, Policy, or Regulation Change Reviewed.	3	3	3	300	350	400	7	11	13	3	4	4	0	26	30	3	4	4	316	398	454
	An IA User-Training Program Provided	913	938	933	1280	1329	1440	1273	1163	1507	970	953	1025	862	790	936	348	244		5646	5417	5841
	IA Personnel Trained.	11	9	12	30	32	32	27	27	32	15	20	20	5	6	6	1	1	1	89	95	103
	An IA Appointment Letter Written and Maintained.	0	1	1	35	45	50	27	27	32	15	20	20	6	7	7	6	6	6	89	106	116
	An IA Memorandum of Agreement/Memorandum of Understanding (MOA/MOU) Maintained.	1	1	2	13	15	15	16	16	18	3	3	4	2	2	2	5	5	5	40	42	46
Workload data in TE 2 GFE	A Software License Maintained.																					
	An IA Report, Recommendation, or Briefing Completed or Meeting Held.	0	3	12		60	66	30	45	60	86	92	90	36	80	80	70	70	70	222	350	378
	IA Information Disseminated.	30	40	50	100	120	140	105	90	100	48	48	48	200	200	300	32	48	48	515	546	686
	An IA Report Prepared	12	12	12	40	50	60	44	55	70	12	12	12	6	6	6	16	18	20	130	153	180
	A Risk Mitigation Recommended	3	1	3	5	10	12	18	20	23	6	6	6	12	12	24	5	8	10	49	57	78
	An IA Inquiry Resolved	180	250	300	300	350	400	4473	4635	4114	3666	3734	3751	3000	3000	3000	1846	2295	2814	13465	14264	14379
	IA Threats and Vulnerabilities Evaluated.	350	400	450	200	220	240	160	386	516	35	50	80	520	780	1040	67	73	80	1332	1909	2406
	A Security Audit, Inspection or Investigation Conducted	0	0	0	2	2	2	5	12	12	4	3	3	6	4	5	2	3	5	19	24	27
Workload data in TE 2 GFE	An audit trail, review, and archive is established and maintained.																					
	An IA Issue Coordinated With Other Agencies.	0	0	0	0	0	0				4	4	4	1	2	2	20	20	20	25	26	26
	An IA Issue Coordinated with COE program.	0	0	0	28	14	24	3	6	6	19	26	20	6	6	6	6	12	18	62	64	74
	A Networkiness Certification Completed.	1	1	1	1	1	1	0	4	3	1	1	2	0	0	0	5	10	8	8	17	15
	A Budget is Executed and Managed.	1	2	2	2	2	2	12	11	13	4	4	4	1	1	1	1	1	1	21	21	23
	IA Procurements Reviewed.	66	82	12	24	24	24	15	18	20	1	1	1	5	10	25	10	10	10	121	145	92
	Participated on Configuration Management Board.	1	2	2	0	0	0	1	1	1	1	1	1	2	2	2	8	8	8	13	14	14
	An IA Inspection Conducted	0	12	12	0	0	0	0	9	9	6	6	6	12	24	24	3	5	10	21	56	61
<b>C.5.4.2.</b>	<b>Manage userIDs and passwords for all systems. Enforce system access, operation, maintenance and disposition in accordance with policies and practices.</b>																					
Workload data in TE 2 C.5.2.7.1	An Unclassified Account, Password, Permission, Inactivity or Suspension Policy Managed.																					
Workload data in TE 2 C.5.2.7.2	A Classified Account, Password, Permission, Inactivity or Suspension Policy Managed.																					
	An IA Personnel Security Clearance Verified.	96	108	108	3	3	3	12	12	12	24	24	24	5	5	5	0	0	0	140	152	152
	A default, guest or services accounts removed, changed or disabled.	900	300	300	50	20	20	81	101	101	323	347	425	20	22	15				1374	790	861
	An Privileged Account Issued.	1	1	1	5	5	5	64	90	95	10	10	10	3	3	3	0	0	0	83	109	114
	A Password Reissued.	24	24	125	370	370	368	614	686	720	82	249	450	4	4	24				1094	1333	1687
	Verification for INFOSEC Training Provided.	0	0	0	60	60	60	9	10	10	24	24	24	4	4	5	0	0	0	97	98	99
	A Password Compliance Tested	0	0	3600	0	0	5000	48	48	48	4	4	4	0	0	0	0	0	0	52	52	8652
	An Illegal Logon Tracked.	0	0	0	24	48	72	24	24	24	0	0	0	520	520	520	0	0	0	568	592	616
	IA Annual Training.															750				0	0	750
<b>C.5.4.3.</b>	<b>Certification and Accreditation</b>																					
	A DITSCAP Approved. Unclass	1	1	1	1	1	1	1	3	4	1	0	1	1	0	1	1	1	1	6	6	9
	A DITSCAP Approved. Class	0	0	1	0	0	0	0	1	1	0	1	1	0	0	0	1	1	1	1	3	4
	A Reaccreditation Approved Unclass	1	0	0				1	1	1	3	0	0	1	0	0	1	1	1	3	2	7
	A Reaccreditation Approved Class	0	0	0				1	0	0	0	0	0	1	0	0	0	1	1	1	1	1

## TECHNICAL EXHIBIT 2 Information Assurance

	An IA Security Tool is Planned and Purchased.	1	1	1	2	3	3	8	8	10	2	4	6	1	1	1				14	17	21
<b>C.5.4.4.</b>	<b>Provide DoD PKI Support</b>																					
	A DoD PKI Supported	0	0	0	0	0	0				0	0	0	0	0	0	0	0	0	0	0	0
	A Common Access Card Authentication Supported.	0	0	24	60	60	1,200	698	126	516	215	472	1,180	10	20	30	0	0	0	983	678	2950
	A Common Access Card device supported. Work Sta	0	0	0	1	1	1	2	2	0	1	1	1	1	1	1				5	5	3
	A Common Access Card device supported. Mobile	0	1	0	0	2	2	0	1	0	0	1	1	0	0	0				0	5	3
	A Common Access Card device supported. Pin Rese	0	0	1	0	1	1	0	2	0	0	0	3	0	2	2				0	5	7
	A CEFMS signature card requested.	246	175	286	378	178	368	171	226	250	139	135	137	188	98	103				1122	812	1144
<b>C.5.4.5.</b>	<b>Perform COMSEC</b>																					
	A COMSEC Inspection Program is Established and Maintained.	1	1	1	1	0	1	0	0	0	1	1	1	0	0	0	1	1	1	4	3	4
	A Sub-Account or Hand Receipt Holder Reviewed. - Sub Account	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1
	A Sub-Account or Hand Receipt Holder Reviewed. - Hand Receipt		0	0	1	1	1	0	0	0	9	36	36	1	0	1				11	37	38
	A Key Vial, U.S. Flag Carrier or Foreign Commercial Aircraft Transported Outside the Continental U.S. Approved.	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	A Waiver to the Grade Restrictions for COMSEC is Submitted and Approved.	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	A Department of Army Cryptographic Access Program is Implemented and Monitored.		0	0		0	0	0	0	0		0	0	0	0	0				0	0	0
	A Department of Army Cryptographic Access Program Point of Contact Designated.	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	A Scheduled Report Provided.	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	A COMSEC Inspector, Custodian and Alternate are Appointed.	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	2	2	2
	A COMSEC Record is Created and Preserved.	0	0	0	8	8	8	0	0	0	0	0	0	1	1	1	8	8	8	17	17	17
	An Employee is Briefed, Certified or Terminated	0	3	2	0	2	0	2	2	2	9	36	36	0	0	0	0	0	0	11	43	40
	A Classified Material is Distributed and Maintained	12	12	12	28	28	28	0	0	0	12	12	12	1	1	1	1	1	1	54	54	54
	A Management Control Reviews Performed.	12	12	12	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	13	13	13
	An Electronic Key Required	12	22	28	12	12	12	4	4	4	3	15	15	8	8	8	10	16	24	49	77	91
	A Sub-Account Established	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	A COMSEC Risk Assessments Conducted.	0	0	0	1	1	1	0	0	0	0	0	0	0	0	0	1	1	1	2	2	2
	An Incident Reported	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	1	0
	A COMSEC Employee Trained.	0	0	2	0	1	0	2	2	2	9	36	47	0	0	0	0	0	0	11	39	51
	An Incident Resolved	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	1	0
<b>C.5.4.6.</b>	<b>Information Assurance Vulnerability Alert (IAVA) Reporting and Compliance (24/7 as required) including Bulletins (IAVB), Technical Tips (IAVTT) and Situational Awareness Reports (SARs)</b>																					
	An IAVA, IAVB, IATT, or SAR notice is coordinated and distributed.	51	82	56	51	82	56	51	82	56	51	82	56	51	82	56	51	82	56	306	492	336
	An IAVA or IAVB is acknowledged.	28	54	72	28	54	72	28	54	72	28	54	72	28	54	72	28	54	72	168	324	432
	An IAVA notice completed and reported to higher headquarters.	21	34	48	21	34	48	21	34	48	21	34	48	21	34	48	21	34	48	126	204	288
	A required scan performed.	46	68	96	46	68	96	46	68	96	46	68	96	46	68	96	46	68	96	276	408	576
	An IA software patch is applied or a configuration change is made and documented.	22800	45600	68400	120000	135000	1560000	126070	158610	177270	125670	133022	128000	20000	21040	25000	0	0	0	414540	493272	1958670
	Populate the Compliance Reporting Database (CRD2) and maintain to current IAVA compliance														979					0	0	979
<b>C.5.4.7.</b>	<b>Monitor and Manage Network Security (24/7 as required)</b>																					

**TECHNICAL EXHIBIT 2  
Information Assurance**

	A network scan completed	3800	7600	11400	240	300	360	1320	1310	1320	156	180	180	1664	1664	2500	0	0	0	7180	11054	15760
	An anomaly reported	48	72	72	48	48	48	120	120	144	95	93	101	0	0	0	0	0	0	311	333	365
	A trend analysis conducted.	0	0	0	2	6	12	60	60	60	2	1	2	0	0	0	0	0	0	64	67	74
	A Security Issue Coordinated	72	84	120	6	6	6	1080	1800	2160	318	263	304	6	6	6				1482	2159	2596
	A Web-page is reviewed for personally identifying (or other inappropriate information)	5000	5400	5800				2900	3988	3500	20991	32429	43289							28891	41817	52589
	A Web-page is reviewed for conformance to the American Disabilities Act (ADA-Section 508 compliance)	2000	2200	2400				300	3988	3500	20991	32429	43289							23291	38617	49189
	A Official or Local Policy Established	0	0	0	3	3	3	10	15	15	24	30	30	1	1	5	0	0	0	38	49	53
	A Firewall system provided.	0	0	0	0	0	0	0	0	0	0	0	11	1	1	1	0	0	0	1	1	12
Workload data in TE 2 GFE	An Antivirus Software system upgraded and updated.																					
	An IDS System Maintained.	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	0	0	0	1	1	2
	A VPN Concentrator Installed	0	0	0	0	0	1	1	1	1	0	0	1	0	0	0	0	0	0	1	1	3
	A Physical Restricted Area Policy Enforced.	1	1	1	6	6	4	5	5	5	99	108	108	8	8	8	0	0	0	119	128	126
	A Physical Restricted Area Policy Enforced.	1	1	1	2	2	1	0	0	0	3	12	12	1	1	1				7	16	15
	An enclave is established.	28	28	28	40	40	38	13	13	13	0	0	0	0	0	0	0	0	0	81	81	79
	An enclave is established.	4	4	4	2	2	1	0	0	0	1	0	0	0	0	0	0	0	0	7	6	5
	A Remote Access Server (RAS) Managed.	1	1	1	2	2	2	3	3	3	12	12	12	1	1	1				19	19	19
	A Wireless Access Concentrator Maintained.	0	0	1	0	0	2	0	0	5	0	0	31	0	0	1	0	0	0	0	0	40
	A wireless security review is conducted	2	2	2				0	0	0	0	0	4							0	2	6
	An Internet Filtering Software System Maintained.	0	0	0	1	1	1	12	12	12	0	0	11	48	48	48	0	0	0	61	61	72
	An Intrusion Test Performed.	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	1	0	1
	An Anti-Spam, Spyware and Adware System Maintained. Unclassified	0	0	0	24	24	24	7204	7464	7600	0	0	10	1	6	6	0	0	0	7229	7494	7640
	An Anti-Spam, Spyware and Adware System Maintained. Classified	0	0	0																0	0	0
<b>C.5.4.8.</b>	<b>Security Incidents</b>																					
	A Security Incident Reported.	3	0	0	0	0	0				0	0	0	0	0	0	2	0	4	5	0	4
	An Incident Log History Provided.	1	1	1	2	2	4	0	0	0	0	0	4	0	1	2	0	0	0	3	4	11
	A virus is found and removed.	2	3	4				13	10	15	53	13	8							68	26	27
	A Device Purged.	300	300	300	9	9	9	12	7	12	4	0	0	75	180	120			0	400	496	441
	An IA Incident Processed.	1	1	1	9	9	9	27	10	30	2	0	0	1	0	0	0	0	0	40	20	40
<b>C.5.4.9.</b>	<b>SA / IASO responsibilities</b>																					
	A Hard Drive Wiped.	300	324	324	360	360	360	305	334	331	560	1,493	1,477	83	235	240	0	0	0	1608	2746	2732
	A New System Evaluated	300	300	300	96	96	96	86	76	93	4	4	6	200	200	200	0	0	0	686	676	695
<b>C.5.4.10.</b>	<b>A System Backup Completed</b>	1200	1200	1200	576	576	600	7956	7956	7956	11068	9982	11050	24	24	24	0	0	0	20824	19738	20830

## TECHNICAL EXHIBIT 2 Information Assurance

PARAGRAPH NUMBER	TITLE	CEPOA			CEPOH			CEPOD			CEPOD TOTALS		
		FY03	FY04	FY05	FY03	FY04	FY05	FY03	FY04	FY05	FY03	FY04	FY05
<b>C.5.4</b>	<b>INFORMATION ASSURANCE</b>												
<b>C.5.4.1</b>	<b>Manage Information Assurance Program</b>												
	A Security Program Provided	1	1	1	1	1	1	1	1	1	3	3	3
	An IA Law, Policy, or Regulation Change Reviewed.	10	3	10	13	18	25	2	3	2	25	24	37
	An IA User-Training Program Provided	678	682	712	468	439	497	121	102	158	1267	1223	1367
	IA Personnel Trained.	2	2	2	14	30	30	2	1	1	18	33	33
	An IA Appointment Letter Written and Maintained.	2	2	2	14	30	30	4	4	4	20	36	36
	An IA Memorandum of Agreement/Memorandum of Understanding (MOA/MOU) Maintained.	2	5	5	2	2	2	1	2	2	5	9	9
Workload data in TE-2 GFE	A Software License Maintained.												
	An IA Report, Recommendation, or Briefing Completed or Meeting Held.	20	24	30	272	291	310	20	25	25	312	340	365
	IA Information Disseminated.	18	24	30	117	118	121	10	12	12	145	154	163
	An IA Report Prepared	28	32	50	35	45	57	48	48	48	111	125	155
	A Risk Mitigation Recommended	4	5	8	30	35	40	2	2	2	36	42	50
	An IA Inquiry Resolved	100	120	140	3,094	4,212	4,738	48	48	48	3242	4380	4926
	IA Threats and Vulnerabilities Evaluated.	50	60	70	360	400	410	48	48	48	458	508	528
	A Security Audit, Inspection or Investigation Conducted	3	3	3	15	15	17	4	4	4	22	22	24
Workload data in TE-2 GFE	An audit trail, review, and archive is established and maintained.												
	An IA Issue Coordinated With Other Agencies.	20	20	20	9	9	9	6	6	6	35	35	35
	An IA Issue Coordinated with COE program.	84	96	108	360	720	720	12	12	12	456	828	840
	A Networkiness Certification Completed.	1	1	1	0	0	0	0	0	1	1	1	2
	A Budget is Executed and Managed.	2	2	2	3	3	3	2	2	2	7	7	7
	IA Procurements Reviewed.	1	3	3	506	580	606	1	1	1	508	584	610
	Participated on Configuration Management Board.	0	3	3	4	5	5	4	4	4	8	12	12
	An IA Inspection Conducted	1	1	1	15	15	17	4	4	4	20	20	22
<b>C.5.4.2.</b>	<b>Manage userIDs and passwords for all systems. Enforce system access, operation, maintenance and disposition in accordance with policies and practices.</b>												
Workload data in TE-2 C.5.2.7.1	An Unclassified Account, Password, Permission, Inactivity or Suspension Policy Managed.												
Workload data in TE-2 C.5.2.7.2	A Classified Account, Password, Permission, Inactivity or Suspension Policy Managed.												
	An IA Personnel Security Clearance Verified.	6	8	4	108	132	132	4	4	4	118	144	140
	A default, guest or services accounts removed, changed or disabled.	0	925	0	268	254	260	3	6	3	271	1185	263
	An Privileged Account Issued.	16	20	18	2	24	2	2	2	2	20	46	22
	A Password Reissued.	96	240	312	24	258	250	36	36	36	156	534	598
	Verification for INFOSEC Training Provided.	6	6	6	507	431	428	1	1	1	514	438	435
	A Password Compliance Tested	2	2	2	986	826	1660	0	0	0	988	828	1662
	An Illegal Logon Tracked.	0	348	0	5592	5472	3312	24	24	24	5616	5844	3336
	IA Annual Training.										0	0	0

## TECHNICAL EXHIBIT 2 Information Assurance

<b>C.5.4.3.</b>	<b>Certification and Accreditation</b>												
	A DITSCAP Approved. Unclass	1	0	1	0	1	1	2	2	2	3	3	4
	A DITSCAP Approved. Class	0	0	1	1	1	1	1	1	1	2	2	3
	A Reaccreditation Approved Unclass	0	0	1	0	0	0	1	1	1	1	1	2
	A Reaccreditation Approved Class						1				0	0	1
	An IA Security Tool is Planned and Purchased.	3	5	6	5	6	8	2	2	2	10	13	16
<b>C.5.4.4.</b>	<b>Provide DoD PKI Support</b>												
	A DoD PKI Supported	0	0	0	0	0	0	0	0	0	0	0	0
	A Common Access Card Authentication Supported.	156	132	180	40	20	250	0	0	0	196	152	430
	A Common Access Card device supported. Work Station	0	0	0	0	0	0	0	0	0	0	0	0
	A Common Access Card device supported. Mobile	0	0	0	0	0	0	0	0	0	0	0	0
	A Common Access Card device supported. Pin Reset	0	0	1	0	0	0	0	0	0	0	0	1
	A CEFMS signature card requested.	269	317	292	200	100	120	66	33	33	535	450	445
<b>C.5.4.5.</b>	<b>Perform COMSEC</b>												
	A COMSEC Inspection Program is Established and Maintained.	1	1	1	4	4	4	0	0	0	5	5	5
	A Sub-Account or Hand Receipt Holder Reviewed. - Sub Account	0	0	0	0	0	0	0	0	0	0	0	0
	A Sub-Account or Hand Receipt Holder Reviewed. - Hand Receipt	0	0	0	0	0	0				0	0	0
	A Key Vial, U.S. Flag Carrier or Foreign Commercial Aircraft Transported Outside the Continental U.S. Approved.	0	0	0	0	0	0	0	0	0	0	0	0
	A Waiver to the Grade Restrictions for COMSEC is Submitted and Approved.	0	0	0	0	0	0	0	0	0	0	0	0
	A Department of Army Cryptographic Access Program is Implemented and Monitored.		0	0		0	0		0	0	0	0	0
	A Department of Army Cryptographic Access Program Point of Contact Designated.	0	0	0	0	0	0	0	2	2	0	2	2
	A Scheduled Report Provided.	0	0	0	0	0	0	0	0	0	0	0	0
	A COMSEC Inspector, Custodian and Alternate are Appointed.	0	0	0	0	0	0	0	0	0	0	0	0
	A COMSEC Record is Created and Preserved.	0	0	0	365	366	365	365	366	365	730	732	730
	An Employee is Briefed, Certified or Terminated	4	4	4	1	1	1	18	18	18	23	23	23
	A Classified Material is Distributed and Maintained	4	4	4	0	0	0	0	0	0	4	4	4
	A Management Control Reviews Performed.	0	0	0	0	0	0	0	0	0	0	0	0
	An Electronic Key Required	18	18	18	1	1	2	18	18	20	37	37	40
	A Sub-Account Established	0	0	0	0	0	0	0	0	0	0	0	0
	A COMSEC Risk Assessments Conducted.	0	6	12	0	0	0	0	0	0	0	6	12
	An Incident Reported	0	0	0	0	0	0	0	0	0	0	0	0
	A COMSEC Employee Trained.	2	2	2	0	0	0	0	0	0	2	2	2
	An Incident Resolved	2	1	0	0	0	0	0	0	0	2	1	0
<b>C.5.4.6.</b>	<b>Information Assurance Vulnerability Alert (IAVA) Reporting and Compliance (24/7 as required) including Bulletins (IAVB), Technical Tips (IAVTT) and Situational Awareness Reports (SARs)</b>												
	An IAVA, IAVB, IATT, or SAR notice is coordinated and distributed.	51	82	56	51	82	56	51	82	56	153	246	168

## TECHNICAL EXHIBIT 2 Information Assurance

	An IAVA or IAVB is acknowledged.	28	54	72	28	54	72	28	54	72	84	162	216
	An IAVA notice completed and reported to higher headquarters.	21	34	48	21	34	48	21	34	48	63	102	144
	A required scan performed.	46	68	96	46	68	96	46	68	96	138	204	288
	An IA software patch is applied or a configuration change is made and documented.	3460	3460	3460	138,183	134,248	133,428	4240	5300	5830	145883	143008	142718
	Populate the Compliance Reporting Database (CRD2) and maintain to current IAVA compliance										0	0	0
<b>C.5.4.7.</b>	<b>Monitor and Manage Network Security (24/7 as required)</b>												
	A network scan completed	36	48	60	152	158	144	88	88	88	276	294	292
	An anomaly reported	20	20	20	4	1	1	10	10	10	34	31	31
	A trend analysis conducted.	0	0	0	84	84	96	0	0	0	84	84	96
	A Security Issue Coordinated	36	36	36	45	36	48	4	4	4	85	76	88
	A Web-page is reviewed for personally identifying (or other inappropriate information)	1560	7060	4000	1700	1951	2000	0	638	638	3260	9649	6638
	A Web-page is reviewed for conformance to the American Disabilities Act (ADA-Section 508 compliance)	1560	7060	4000	1700	1951	2000	0	638	638	3260	9649	6638
	A Official or Local Policy Established	72	72	72	3,441	2,905	2,705	4	4	4	3517	2981	2781
	A Firewall system provided.	5	5	5	0	0	0	0	0	0	5	5	5
Workload data in TE-2 GFE	An Antivirus Software system upgraded and updated.												
	An IDS System Maintained.	0	0	0	0	0	0	0	0	0	0	0	0
	A VPN Concentrator Installed	1	1	1	0	2	3	4	4	4	5	7	8
	A Physical Restricted Area Policy Enforced.	1	1	1	120	120	120	2	2	2	123	123	123
	A Physical Restricted Area Policy Enforced.	1	1	1	12	12	12	1	1	1	14	14	14
	An enclave is established.	2	2	2	0	0	0	2	2	2	4	4	4
	An enclave is established.	1	1	1	0	0	0	1	1	1	2	2	2
	A Remote Access Server (RAS) Managed.	2	2	1	1	3	3	1	1	1	4	6	5
	A Wireless Access Concentrator Maintained.	0	0	0	0	0	0	0	3	3	0	3	3
	A wireless security review is conducted	0	0	0	0	0	0	0	0	4	0	0	4
	An Internet Filtering Software System Maintained.	1	1	1	0	0	0	0	2	2	1	3	3
	An Intrusion Test Performed.	2	2	2	0	0	0	4	4	4	6	6	6
	An Anti-Spam, Spyware and Adware System Maintained. Unclassified	2	2	750	0	32	60	3	4	4	5	38	814
	An Anti-Spam, Spyware and Adware System Maintained. Classified										0	0	0
<b>C.5.4.8.</b>	<b>Security Incidents</b>												
	A Security Incident Reported.	0	0	0	0	0	0	0	0	0	0	0	0
	An Incident Log History Provided.	0	1	2	1	0	2	0	2	1	1	3	5
	A virus is found and removed.	25	10	5	4	0	1	8	2	2	37	12	8
	A Device Purged.	0	9	0	9	8	24	0	4	4	9	21	28
	An IA Incident Processed.	5	5	5	4	1	3	0	1	1	9	7	9
<b>C.5.4.9.</b>	<b>SA / IASO responsibilities</b>												
	A Hard Drive Wiped.	0	0	0	215	165	144	0	94	103	215	259	247
	A New System Evaluated	0	67	213	310	240	240	0	29	24	310	336	477
<b>C.5.4.10.</b>	<b>A System Backup Completed</b>	2808	2808	2808	12,880	10,015	10,015	884	884	936	16572	13707	13759

**TECHNICAL EXHIBIT 2  
Information Assurance**

PARAGRAPH NUMBER	TITLE	CESAC			CESAJ			CESAJCERP			CESAJMJC			CESAM			CESAS			CESAW			CESAD			CESAD TOTALS			
		FY03	FY04	FY05	FY03	FY04	FY05	FY03	FY04	FY05	FY03	FY04	FY05	FY03	FY04	FY05	FY03	FY04	FY05	FY03	FY04	FY05	FY03	FY04	FY05	FY03	FY04	FY05	
<b>C.5.4</b>	<b>INFORMATION ASSURANCE</b>																												
<b>C.5.4.1</b>	<b>Manage Information Assurance Program</b>																												
	A Security Program Provided	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	7	8	8
	An IA Law, Policy, or Regulation Change Reviewed.	1	1	1	1	3	2	0	0	0	0	2	3	25	50	40	10	20	25	5	15	15	17	39	44	59	130	130	
	An IA User-Training Program Provided	159	145	165	1066	1189	1235						1483	1589	1697	1044	1055	1177	714	429	436	151	97	151	4617	4504	4861		
	IA Personnel Trained.	1	1	1	18	18	18	0	0	0	0	1	1	7	7	18	16	16	16	3	3	5	4	5	5	49	51	64	
	An IA Appointment Letter Written and Maintained.	5	5	5	6	6	6	0	0	0	0	1	1	7	7	7	15	15	15	7	7	7	5	6	6	45	47	47	
	An IA Memorandum of Agreement/Memorandum of Understanding (MOA/MOU) Maintained.	2	2	2	2	3	2	0	0	0	0	0	1	8	10	12	5	1	3	4	4	4	1	3	3	22	23	27	
Workload data in TE 2 GFE	A Software License Maintained.																												
	An IA Report, Recommendation, or Briefing Completed or Meeting Held.	0	0	0	60	60	60	0	0	0	0	0	152	120	120	120	80	77	90	52	63	66	40	60	80	352	380	568	
	IA Information Disseminated.	200	200	200	263	522	544	0	0	0	0	0	152	120	160	200	200	300	100	13	28	28	12	12	12	808	1222	1236	
	An IA Report Prepared	6	6	6	28	55	65	0	0	0	0	0	12	36	60	48	30	35	35		30	27	6	8	8	106	194	201	
	A Risk Mitigation Recommended	2	2	2	3	1	2	0	0	0	0	0	104	6	6	6	25	18	10	5	15	15	27	30	35	68	72	174	
	An IA Inquiry Resolved	20	20	20	3208	3553	4280	0	0	0	0	200	700	750	850	800	500	800	1250	24	36	32	24	30	36	4526	5489	7118	
	IA Threats and Vulnerabilities Evaluated	150	200	300	4286	4800	5720	0	0	0	0	52	52	200	300	400	250	400	300		132	132	130	139	160	5016	6023	7064	
	A Security Audit, Inspection or Investigation Conducted	1	1	1	65	75	80	0	0	0	0	30	52	13	18	23	10	12	11		10	10	4	4	4	93	150	181	
Workload data in TE 2 GFE	An audit trail, review, and archive is established and maintained.																												
	An IA Issue Coordinated With Other Agencies.	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	2	3	2	2	3	
	An IA Issue Coordinated with COE program.	2	2	2	3	3	1	4	8	6	3	3	17	20	30	30	20	20	20	0	4	4	2	3	2	54	73	82	
	A Network Certification Completed.	1	1	1	1	1	1	1	1	1	0	1	1	5	7	5	5	5	0	0	0	0	1	7	9	15	23		
	A Budget is Executed and Managed.	1	1	1	1	1	1				0	2	2	1	1	1	1	1	1	1	1	1	2	2	2	7	9	9	
	IA Procurements Reviewed.	1	1	1	1	1	1	1	1	1	1	2	1	3	5	7	15	10	15		1	1	5	5	6	27	26	33	
	Participated on Configuration Management Board.	1	1	1	0	1	1				0	0	0	5	5	5	2	2	2	1	2	2	2	2	2	11	13	13	
	An IA Inspection Conducted	2	2	2	12	12	12	0	0	0	0	0	12	5	7	16	480	960			16	48	2	2	4	501	999	94	
<b>C.5.4.2.</b>	<b>Manage userIDs and passwords for all systems. Enforce system access, operation, maintenance and disposition in accordance with policies and practices.</b>																												
Workload data in TE 2 C.5.2.7.1	An Unclassified Account, Password, Permission, Inactivity or Suspension Policy Managed.																												
Workload data in TE 2 C.5.2.7.2	A Classified Account, Password, Permission, Inactivity or Suspension Policy Managed.																												
	An IA Personnel Security Clearance Verified	7	7	7	108	108	120	0	0	0	12	12	12	7	7	7	15	15	15	0	6	1	4	5	5	153	160	167	
	A default, guest or services accounts removed, changed or disabled.	150	100	40	0	0	0	29	42	60	0	94	210	600	450	500	1800	2000	2100		488	100	60	78	56	2639	3252	3066	
	An Privileged Account Issued.	5	1	3	26	36	39	14	19	12	1	5	5	38	41	38	20	20	20	9	10	10	6	6	6	119	138	133	
	A Password Reissued.	2	3	2	42	86	180	275	375	540	192	120	180	252	612	795	120	180	120	1	2	12	2	3	64	886	1381	1893	
	Verification for INFOSEC Training Provided.	0	0	0	0	0	0	0	0	0	0	0	0	36	60	60	204	120	240	4	4	4	2	3	6	246	187	310	
	A Password Compliance Tested	0	0	0	12	12	10	12	12	12	9	9	9	6	6	0	30	40	25	0	42	80	10	10	10	79	131	146	
	An Illegal Logon Tracked.	2400	2400	2400	96	96	100	0	0	0	0	0	960	24	198	108	60	60	24	48	64	96	12	12	12	2640	2830	3700	
	IA Annual Training.																									0	0	0	
<b>C.5.4.3.</b>	<b>Certification and Accreditation</b>																												
	A DITSCAP Approved. Unclass	0	1	0	1	1	1						1	1	1	1	1	2	0	1	1	0	2	7	3	7	12		
	A DITSCAP Approved. Class				1	1	1						1	1	1	1	1	2	0	0	1	0	0	0	3	3	5		
	A Reaccreditation Approved Unclass	0	0	1	1	0	0						0	0	1	0	0	1		1	1	0	0	2	1	1	6		
	A Reaccreditation Approved Class				0	1	0						0	1	1	15	10	15								15	12	16	
	An IA Security Tool is Planned and Purchased.	3	3	3	2	3	4				0	0	6	10	10	12				2	2	4	6	7	19	24	34		
<b>C.5.4.4.</b>	<b>Provide DoD PKI Support</b>																												
	A DoD PKI Supported	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
	A Common Access Card Authentication Supported.	0	30	3	0	1006	425	0	0	0	0	0	0	115	176	312	0	25	25	1	2	12	6	4	15	122	1243	792	
	A Common Access Card device supported. Work Sta	0	0	0	0	0	0						1	1	0		1	0		1	1				1	3	1		
	A Common Access Card device supported. Mobile	0	1	1	0	3	1						0	1	1		0	0							0	5	3		
	A Common Access Card device supported. Pin Rese	0	0	0	0	2	2						0	5	5		0	0							0	7	7		
	A CEFMS signature card requested.	50	50	50	104	88	120						213	208	210	350	350	350	82	73	145				799	769	875		
<b>C.5.4.5.</b>	<b>Perform COMSEC</b>																												
	A COMSEC Inspection Program is Established and Maintained.	0	0	0	1	1	1	0	0	0	0	0	0	1	1	1	2	3	2	0	0	0	0	0	0	4	5	4	

**TECHNICAL EXHIBIT 2  
Information Assurance**

	A Sub-Account or Hand Receipt Holder Reviewed. - Sub Account	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	0	0	0	1	1	1	
	A Sub-Account or Hand Receipt Holder Reviewed. - Hand Receipt	0	0	0	1	1	1						1	1	1	0	0	0	0	0	0	1	1	1	3	3	3		
	A Key Vial, U.S. Flag Carrier or Foreign Commercial Aircraft Transported Outside the Continental U.S. Approved.	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	
	A Waiver to the Grade Restrictions for COMSEC is Submitted and Approved.	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
	A Department of Army Cryptographic Access Program is Implemented and Monitored.	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
	A Department of Army Cryptographic Access Program Point of Contact Designated.	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1
	A Scheduled Report Provided.	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	A COMSEC Inspector, Custodian and Alternate are Appointed.	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	A COMSEC Record is Created and Preserved.	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	An Employee is Briefed, Certified or Terminated	0	0	0	5	5	5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	A Classified Material is Distributed and Maintained	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	A Management Control Reviews Performed.	0	0	0	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	An Electronic Key Required	0	0	0	12	12	12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	A Sub-Account Established	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	A COMSEC Risk Assessments Conducted.	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	An Incident Reported	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	A COMSEC Employee Trained.	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	An Incident Resolved	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
<b>C.5.4.6.</b>	<b>Information Assurance Vulnerability Alert (IAVA) Reporting and Compliance (24/7 as required) including Bulletins (IAB), Technical Tips (IAVTT) and Situational Awareness Reports (SARs)</b>																												
	An IAVA, IAVB, IATT, or SAR notice is coordinated and distributed.	51	82	56	51	82	56	51	82	56	51	82	56	51	82	56	51	82	56	51	82	56	51	82	56	408	656	448	
	An IAVA or IAVB is acknowledged.	28	54	72	28	54	72	28	54	72	28	54	72	28	54	72	28	54	72	28	54	72	28	54	72	224	432	576	
	An IAVA notice completed and reported to higher headquarters.	21	34	48	21	34	48	21	34	48	21	34	48	21	34	48	21	34	48	21	34	48	21	34	48	168	272	384	
	A required scan performed.	46	68	96	46	68	96	46	68	96	46	68	96	46	68	96	46	68	96	46	68	96	46	68	96	368	544	768	
	An IA software patch is applied or a configuration change is made and documented.	500	500	500	148666	265728	264000	0	0	0	144	144	216	96000	#####	#####	30000	30000	30000										
	Populate the Compliance Reporting Database (CRD2) and maintain to current IAVA compliance																												
<b>C.5.4.7.</b>	<b>Monitor and Manage Network Security (24/7 as required)</b>																												
	A network scan completed	9	9	9	828	828	828	0	0	4	0	0	450	480	480	600	730	730	730	0	421	421	14	14	24	2061	2482	3066	
	An anomaly reported	4	4	4	1	2	0	4	4	4	1	2	144	0	6	6	500	800	700	3	4	6	15	24	25	528	846	889	
	A trend analysis conducted.	3	3	3	12	12	12	0	0	48	12	12	12	6	8	10	0	0	0	0	0	0	0	1	2	4	34	37	89
	A Security Issue Coordinated	5	5	5	41	49	48	12	12	12	0	0	96	12	12	12	12	12	12	36	36	36	6	8	8	124	134	229	
	A Web-page is reviewed for personally identifying (or other inappropriate information)				49000	58292	61635				49000	58292	61635	11921	17451	18728	14560	19660	24360	90	176	132				124571	153871	166490	
	A Web-page is reviewed for conformance to the American Disabilities Act (ADA-Section 508 compliance)				49000	58292	61635				49000	58292	61635	5961	8726	9364	14560	19660	24360	90	176	132				118611	145146	157126	
	A Official or Local Policy Established	5	20	15	59	67	66	2	12	12	2	9	12	10	10	8	20	6	3	9	9	9	13	20	30	120	153	155	
	A Firewall system provided.	0	0	0	12	24	36	36	27	48	0	0	12	0	0	0	0	0	0	0	0	0	0	0	0	2	48	51	98
Workload data in TE 2 GFE	An Antivirus Software system upgraded and updated.																200	200	200					200	200	200			
	An IDS System Maintained.	0	0	0	36	36	48	0	0	24	0	0	12	1	1	1	0	2	22	0	0	0	0	0	0	1	37	39	108
	A VPN Concentrator Installed	0	0	0	3	0	12	12	0	0	0	0	12	0	0	0	0	0	1	0	3	12	0	0	1	0	15	41	
	A Physical Restricted Area Policy Enforced.	1	1	1	228	228	228	12	12	12	36	48	48	3	3	3	3	3	3	6	6	6	2	2	3	291	303	304	
	A Physical Restricted Area Policy Enforced.	0	0	0	0	0	0	0	0	0	0	0	0	1	2	2	1	2	2	1	1	1	1	1	1	4	6	6	
	An enclave is established.	1	1	1	36	36	36	0	0	0	36	48	48	1	1	1	0	0	6	12	12	12	1	1	1	1	87	99	105
	An enclave is established.	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	0	12								13	25	13	
	A Remote Access Server (RAS) Managed.	1	1	1	12	12	12	0	0	0	0	0	0	1	1	1	2	2	2	12	12	12				28	28	28	
	A Wireless Access Concentrator Maintained.	0	0	0	0	27	36	0	0	0	0	0	0	0	0	1	0	0	7	24	24	60	0	0	10	24	51	114	
	A wireless security review is conducted				0	104	104				0	104	104	0	0	1	0	0	50	4	4	4				4	212	263	
	An Internet Filtering Software System Maintained.	1	1	1	0	0	12	0	0	0	0	0	0	0	0	0	0	12	12	12	12	12	12	0	1	1	25	26	38
	An Intrusion Test Performed.	1	1	1	0	3	2	0	0	0	0	0	0	3	0	0	0	4	4	4	0	4	4	2	2	4	7	14	18

**TECHNICAL EXHIBIT 2  
Information Assurance**

	An Anti-Spam, Spyware and Adware System Maintained. Unclassified	1	1	1	0	3060	3060	0	0	0	0	0	240	36	36	24	200	200	200	0	154	154	10	11	24	247	3462	3703	
	An Anti-Spam, Spyware and Adware System Maintained. Classified																									0	0	0	
<b>C.5.4.8.</b>	<b>Security Incidents</b>																												
	A Security Incident Reported.	0	0	0	0	0	1	0	0	0	0	0	0	0	1	0	0	0	4	0	0	0	0	0	4	0	1	9	
	An Incident Log History Provided.	0	0	0	0	0	0	0	0	0	0	24	96	84	36	36	1	3	0	0	6	4	0	0	0	85	69	136	
	A virus is found and removed.				38	112	50					38	112	50	160	61	16	2	3	2		36	36				238	324	154
	A Device Purged.	0	0	0	0	0	0						240	84	12	24	35	5	5	0	2	0			4	119	19	273	
	An IA Incident Processed.	0	0	0	0	0	0	0	0	0	0	24	60	48	48	30	30	30	12	18	12	1	1	4	103	97	118		
<b>C.5.4.9.</b>	<b>SA / IASO responsibilities</b>																												
	A Hard Drive Wiped.	40	50	50	167	219	240	0	0	0	0	24	591	544	550	200	400	200	100	137	160	29	124	71	1127	1474	1295		
	A New System Evaluated	40	50	50	305	441	318	0	7	60	30	44	228	428	487	430	30	50	20	0	4	8	60	50	75	893	1133	1189	
<b>C.5.4.10.</b>	<b>A System Backup Completed</b>	20	20	20	37200	39600	43200	745	840	912	2268	2160	3024	600	704	832	23725	23725	23725	10529	10529	10529	52	52	52	75139	77630	82294	

## TECHNICAL EXHIBIT 2 Information Assurance

PARAGRAPH NUMBER	TITLE	CESPA			CESPK			CESPL			CESPN			CESPD			CESPD TOTALS		
		FY03	FY04	FY05	FY03	FY04	FY05	FY03	FY04	FY05									
<b>C.5.4</b>	<b>INFORMATION ASSURANCE</b>																		
<b>C.5.4.1</b>	<b>Manage Information Assurance Program</b>																		
	A Security Program Provided	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	5	5	5
	An IA Law, Policy, or Regulation Change Reviewed.	0	8	11	46	46	56	40	40	40	15	95	120	8	15	13	109	204	240
	An IA User-Training Program Provided	417	388	443	1227	1010	1150	811	826	948	317	390	449	139	110	101	2911	2724	3091
	IA Personnel Trained.	3	8	10	28	24	26	8	8	8	6	6	7	2	3	3	47	49	54
	An IA Appointment Letter Written and Maintained.	6	6	6	28	47	26	2	2	2	6	6	7	2	3	3	44	64	44
	An IA Memorandum of Agreement/Memorandum of Understanding (MOA/MOU) Maintained.	3	5	5	13	15	17	25	25	25	1	3	3	1	1	1	43	49	51
Workload data in TE 2 GFE	A Software License Maintained.																		
	An IA Report, Recommendation, or Briefing Completed or Meeting Held.	180	180	180	591	740	938	180	180	180	40	60	50	68	52	40	1059	1212	1388
	IA Information Disseminated.	43	43	43	150	139	162	7	7	7	36	48	72	65	77	68	301	314	352
	An IA Report Prepared	32	32	32	66	139	159	26	26	26	31	24	30	10	44	58	165	265	305
	A Risk Mitigation Recommended	365	387	390	592	607	815	169	175	180	120	150	180	3	3	3	1249	1322	1568
	An IA Inquiry Resolved	365	679	917	2225	2572	3094	2970	3000	3100	360	480	720	161	164	156	6081	6895	7987
	IA Threats and Vulnerabilities Evaluated.	365	535	647	4071	4734	5966	140	339	378	273	489	630	0	10010	10010	4849	16107	17631
	A Security Audit, Inspection or Investigation Conducted	8	8	8	7	8	8	11	17	26	2	3	5	2	1	1	30	37	48
Workload data in TE 2 GFE	An audit trail, review, and archive is established and maintained.																		
	An IA Issue Coordinated With Other Agencies.	0	0	0	28	28	35				0	0	0	4	3	2	32	31	37
	An IA Issue Coordinated with COE program.	1	3	3	47	47	62	24	26	30	8	10	14	19	61	42	99	147	151
	A Networthiness Certification Completed.	1	1	1	1	1	1	0	0	2	0	1	1	1	1	1	3	4	6
	A Budget is Executed and Managed.	1	2	1	2	2	2	1	1	1	2	1	2	2	3	3	8	9	9
	IA Procurements Reviewed.	1	1	1	13	25	21	2	2	2	4	3	3	0	0	0	20	31	27
	Participated on Configuration Management Board.	1	1	1	6	5	6	2	2	2	2	2	2	1	3	3	12	13	14
	An IA Inspection Conducted	2	4	11	127	180	239	24	36	36	12	16	16	0	0	0	165	236	302
<b>C.5.4.2.</b>	<b>Manage userIDs and passwords for all systems. Enforce system access, operation, maintenance and disposition in accordance with policies and practices.</b>																		
Workload data in TE 2 C.5.2.7.1	An Unclassified Account, Password, Permission, Inactivity or Suspension Policy Managed.																		
Workload data in TE 2 C.5.2.7.2	A Classified Account, Password, Permission, Inactivity or Suspension Policy Managed.																		
	An IA Personnel Security Clearance Verified.	51	51	51	27	23	24	19	16	16	6	6	7	2	2	2	105	98	100
	A default, guest or services accounts removed, changed or disabled.	579	579	579	972	640	914	273	280	282	140	140	140	0	0	0	1964	1639	1915
	An Privileged Account Issued.	15	18	22	26	22	24	14	21	18	0	0	0	0	0	0	55	61	64
	A Password Reissued.	48	48	48	452	688	905	560	593	58	104	100	100				1164	1429	1111
	Verification for INFOSEC Training Provided.	10	22	30	25	20	22	2	2	2	6	12	12	4	4	4	47	60	70
	A Password Compliance Tested	0	0	0	149	164	164	10	12	15	0	0	0	0	0	0	159	176	179

## TECHNICAL EXHIBIT 2 Information Assurance

	An Illegal Logon Tracked.	2	4	12	0	1	0	3325	3112	3156	5	5	5	0	0	0	3332	3122	3173
	IA Annual Training.																0	0	0
<b>C.5.4.3.</b>	<b>Certification and Accreditation</b>																		
	A DITSCAP Approved. Unclass	0	1	0	1	1	1	1	1	1	0	1	1	0	0	0	2	4	3
	A DITSCAP Approved. Class	0	1	0	1	1	1	1	1	1				1	1	1	3	4	3
	A Reaccreditation Approved Unclass	0	0	0	0	0	1	1	1	1	0	1	1	0	0	0	1	2	3
	A Reaccreditation Approved Class	0	0	0	0	0	1	1	1	1				0	0	0	1	1	2
	An IA Security Tool is Planned and Purchased.	2	2	2	13	23	19	2	2	2	4	3	3	0	0	0	21	30	26
<b>C.5.4.4.</b>	<b>Provide DoD PKI Support</b>																		
	A DoD PKI Supported	0	0	0	0	0	0				0	0	0	0	0	0	0	0	0
	A Common Access Card Authentication Supported.	0	108	4200	23	46	665	0	0	96	0	14	72	0	0	0	23	168	5033
	A Common Access Card device supported. Work Sta	0	0	0	1	1	1	0	0	1				0	0	0	1	1	2
	A Common Access Card device supported. Mobile	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	1	1
	A Common Access Card device supported. Pin Reset	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	A CEFMS signature card requested.	175	175	175	114	323	400	200	205	210	128	113	100	0	0	0	617	816	885
<b>C.5.4.5.</b>	<b>Perform COMSEC</b>																		
	A COMSEC Inspection Program is Established and Maintained.	1	1	1	0	0	0	2	1	2	0	1	3	0	0	0	3	3	6
	A Sub-Account or Hand Receipt Holder Reviewed. - Sub Account	0	0	0	1	1	1	0	0	0	0	0	0	0	0	0	1	1	1
	A Sub-Account or Hand Receipt Holder Reviewed. - Hand Receipt	0	0	0	3	3	10				0	0	0	0	0	0	3	3	10
	A Key Vial, U.S. Flag Carrier or Foreign Commercial Aircraft Transported Outside the Continental U.S. Approved.	0	0	0	0	0	0				0	0	0	0	0	0	0	0	0
	A Waiver to the Grade Restrictions for COMSEC is Submitted and Approved.	0	0	0	0	0	0				0	0	0	0	0	0	0	0	0
	A Department of Army Cryptographic Access Program is Implemented and Monitored.		0	0	0	0	0				0	0	0				0	0	0
	A Department of Army Cryptographic Access Program Point of Contact Designated.	0	0	0	0	0	0				0	0	0	0	0	0	0	0	0
	A Scheduled Report Provided.	0	0	0	0	0	0				0	0	0	0	0	0	0	0	0
	A COMSEC Inspector, Custodian and Alternate are Appointed.	1	1	1	0	0	0	1	1	1	0	0	0	0	0	0	2	2	2
	A COMSEC Record is Created and Preserved.	1	1	1	55	55	55	72	66	72	5	36	36	0	0	0	133	158	164
	An Employee is Briefed, Certified or Terminated	0	0	0	0	0	0	3	3	3	3	3	3	0	0	0	6	6	6
	A Classified Material is Distributed and Maintained	1	1	1	1	1	1	1	1	2	1	1	1	0	0	0	4	4	5
	A Management Control Reviews Performed.	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	2	2	2
	An Electronic Key Required	4	4	4	32	32	32	16	16	16	13	16	16	0	0	0	65	68	68
	A Sub-Account Established	0	0	0	0	0	0				0	0	0	0	0	0	0	0	0
	A COMSEC Risk Assessments Conducted.	1	1	1	2	2	2	1	1	1	1	4	4	0	0	0	5	8	8
	An Incident Reported	0	1	0	0	1	0				0	0	0	0	0	0	0	0	2
	A COMSEC Employee Trained.	0	2	10	4	4	10	5	5	5	1	3	0	0	0	0	10	14	25
	An Incident Resolved	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	2	0

## TECHNICAL EXHIBIT 2 Information Assurance

<b>C.5.4.6.</b>	<b>Information Assurance Vulnerability Alert (IAVA) Reporting and Compliance (24/7 as required) including Bulletins (IAVB), Technical Tips (IAVTT) and Situational Awareness Reports (SARs)</b>																			
	An IAVA, IAVB, IATT, or SAR notice is coordinated and distributed.	51	82	56	51	82	56	51	82	56	51	82	56	51	82	56	255	410	280	
	An IAVA or IAVB is acknowledged.	28	54	72	28	54	72	28	54	72	28	54	72	28	54	72	140	270	360	
	An IAVA notice completed and reported to higher headquarters.	21	34	48	21	34	48	21	34	48	21	34	48	21	34	48	105	170	240	
	A required scan performed.	46	68	96	46	68	96	46	68	96	46	68	96	46	68	96	230	340	480	
	An IA software patch is applied or a configuration change is made and documented.	22,350	25,374	32,000	47742	57995	71662	10983	13944	15432	15,000	24,000	36,000	0	0	0	96075	121313	155094	
	Populate the Compliance Reporting Database (CRD2) and maintain to current IAVA compliance																0	0	0	
<b>C.5.4.7.</b>	<b>Monitor and Manage Network Security (24/7 as required)</b>																			
	A network scan completed	0	412	510	366	582	598	360	384	408	75	150	150	0	0	0	801	1528	1666	
	An anomaly reported	9	15	24	1051	2275	5915	721	1087	540	120	150	180	0	0	0	1901	3527	6659	
	A trend analysis conducted.	12	12	12	67	67	71	32	43	58	52	80	100	8	8	8	171	210	249	
	A Security Issue Coordinated	4	41	45	25,915	28,796	40318	22	31	38	12	24	36	24	24	24	25977	28916	40461	
	A Web-page is reviewed for personally identifying (or other inappropriate information)	6760	6501	2528	19949	18303	24997	7275	7390	7485	1065	1040	1374	2	3	3	35051	33237	36387	
	A Web-page is reviewed for conformance to the American Disabilities Act (ADA-Section 508 compliance)	5408	6176	2528	19949	18203	24997	7275	7390	7485	1065	1040	1374	0	0	0	33697	32809	36384	
	A Official or Local Policy Established	11	14	15	71	73	174	2	2	2	12	13	14	16	34	35	112	136	240	
	A Firewall system provided.	0	0	0	10	17	28	0	0	0	0	0	0	0	0	0	10	17	28	
Workload data in TE 2 GFE	An Antivirus Software system upgraded and updated.																			
	An IDS System Maintained.	0	0	0	3	5	7				0	0	0	0	0	0	3	5	7	
	A VPN Concentrator Installed	0	0	1	1	1	1	2	0	5	0	0	0	0	0	0	3	1	7	
	A Physical Restricted Area Policy Enforced.	18	18	18	48	48	48	2	2	2	4	4	4	0	0	0	72	72	72	
	A Physical Restricted Area Policy Enforced.	1	1	1	36	33	36	1	1	1	1	1	1				39	36	39	
	An enclave is established.	24	28	28	1	1	1	27	27	27	1	1	1	0	0	0	53	57	57	
	An enclave is established.	1	1	1	1	1	1	1	1	1		1	1	0	0	0	3	4	4	
	A Remote Access Server (RAS) Managed.	1	1	1	4	4	4	2	2	2	3	2	2	0	0	0	10	9	9	
	A Wireless Access Concentrator Maintained.	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	1	
	A wireless security review is conducted	0	0	12	1	2	8	0	1	3	0	0	2	0	0	2	1	3	27	
	An Internet Filtering Software System Maintained.	1	1	1	12	12	18	0	0	0	1	1	1	0	0	0	14	14	20	
	An Intrusion Test Performed.	0	0	0	0	0	0	2	1	2	1	0	1	0	0	0	3	1	3	
	An Anti-Spam, Spyware and Adware System Maintained. Unclassified	350	350	350	0	38882	115804	192	192	192	0	120	240	0	0	0	542	39544	116586	
	An Anti-Spam, Spyware and Adware System Maintained. Classified																0	0	0	
<b>C.5.4.8.</b>	<b>Security Incidents</b>																			
	A Security Incident Reported.	0	0	0	0	0	0				0	0	0	0	0	1	0	0	1	
	An Incident Log History Provided.	4	4	4	6	7	8	4	4	4	0	0	0	0	0	0	14	15	16	
	A virus is found and removed.	75	125	125	1,221	3,037	6,075	532	592	610	25	0	0	0	0	0	1853	3754	6810	

## TECHNICAL EXHIBIT 2 Information Assurance

	A Device Purged.	1	1	4	107	115	180	24	24	24	125	100	100	0	0	0	257	240	308
	An IA Incident Processed.	12	12	12	2	0	1	12	12	12	2	3	5	4	4	4	32	31	34
<b>C.5.4.9.</b>	<b>SA / IASO responsibilities</b>																		
	A Hard Drive Wiped.	124	312	367	257	359	460	90	82	82	190	146	216	0	0	0	661	899	1125
	A New System Evaluated	204	144	125	980	1166	138	25	25	340	250	325	320	25	10	30	1484	1670	953
<b>C.5.4.10.</b>	A System Backup Completed	2107	2502	2945	3,396	8,104	9,370	6,370	6,370	6370	16950	16950	16950	0	0	0	28823	33926	35634.5

## TECHNICAL EXHIBIT 2 Information Assurance

PARAGRAPH NUMBER	TITLE	CESWF			CESWG			CESWL			CESWT			CESWD			CESWD TOTALS		
		FY03	FY04	FY05	FY03	FY04	FY05	FY03	FY04	FY05	FY03	FY04	FY05	FY03	FY04	FY05	FY03	FY04	FY05
<b>C.5.4</b>	<b>INFORMATION ASSURANCE</b>																		
<b>C.5.4.1</b>	<b>Manage Information Assurance Program</b>																		
	A Security Program Provided	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	4	4	4
	An IA Law, Policy, or Regulation Change Reviewed.	2	30	24	13	29	12	40	40	40	15	25	30	0	1	1	30	85	67
	An IA User-Training Program Provided	1128	997	1186	421	432	517	1124	808	913	1014	810	901	129	103	109	2692	2342	2713
	IA Personnel Trained.	3	0	5	2	9	6	8	8	8	5	6	7	1	1	1	11	16	19
	An IA Appointment Letter Written and Maintained.	4	4	4	16	6	7	2	2	2	8	8	8	5	5	10	33	23	29
	An IA Memorandum of Agreement/Memorandum of Understanding (MOA/MOU) Maintained.	1	3	3	0	0	0	25	25	25	3	3	3	2	7	7	6	13	13
Workload data in TE 2 GFE	A Software License Maintained.																		
	An IA Report, Recommendation, or Briefing Completed or Meeting Held.	45	35	50	229	326	422	180	180	180	60	60	80	290	86	52	624	507	604
	IA Information Disseminated.	10	13	26	8	8	8	7	7	7	8	8	8	13	13	13	39	42	55
	An IA Report Prepared	20	10	5	67	71	80	26	26	26	20	20	30	290	86	52	397	187	167
	A Risk Mitigation Recommended	2	19	22	20	40	15	169	175	180	12	15	10	0	0	0	34	74	47
	An IA Inquiry Resolved	20	10	5	130	238	320	2,970	3,000	3,100	200	300	350	218	218	218	568	766	893
	IA Threats and Vulnerabilities Evaluated.	20	40	40	263	379	475	140	339	378	101	176	228	260	260	260	644	855	1003
	A Security Audit, Inspection or Investigation Conducted	3	3	3	30	15	16	11	17	26	1	1	1	4	4	2	38	23	22
Workload data in TE 2 GFE	An audit trail, review, and archive is established and maintained.																		
	An IA Issue Coordinated With Other Agencies.	0	2	2	0	0	0	0	0	0	0	0	0	8	8	8	8	10	10
	An IA Issue Coordinated with COE program.	10	9	10	31	28	18	24	26	30	2	2	3	48	48	96	91	87	127
	A Networkiness Certification Completed.	0	0	0	0	0	0	0	0	0	2	0	0	1	0	0	0	0	1
	A Budget is Executed and Managed.	2	2	2	0	0	0	1	1	1	2	2	2	1	1	1	5	5	5
	IA Procurements Reviewed.	1	2	2	1	1	1	2	2	2	1	1	1	1	1	1	4	5	5
	Participated on Configuration Management Board.	3	3	3	0	0	0	2	2	2	0	0	0	2	2	2	5	5	5
	An IA Inspection Conducted	12	12	12	480	480	480	24	36	36	4	6	6	52	52	52	548	550	550
<b>C.5.4.2.</b>	<b>Manage userIDs and passwords for all systems. Enforce system access, operation, maintenance and disposition in accordance with policies and practices.</b>																		
Workload data in TE 2 C.5.2.7.1	An Unclassified Account, Password, Permission, Inactivity or Suspension Policy Managed.																		
Workload data in TE 2 C.5.2.7.2	A Classified Account, Password, Permission, Inactivity or Suspension Policy Managed.																		
	An IA Personnel Security Clearance Verified.	8	8	8	156	102	60	19	16	16	6	7	7	2	2	2	172	119	77
	A default, guest or services accounts removed, changed or disabled.	1000	500	500	155	110	150	273	280	282	300	800	400	113	113	120	1568	1523	1170
	An Privileged Account Issued.	40	28	25	5	5	5	14	21	18	5	6	7	4	4	4	54	43	41
	A Password Reissued.	50	75	85		15	120	560	593	58	100	100	200	0	20	60	150	210	465
	Verification for INFOSEC Training Provided.	1	2	2	2	8	6	2	2	2	8	8	8	0	0	2	11	18	18
	A Password Compliance Tested	0	12	12	0	0	0	10	12	15	0	0	0	0	1	1	0	13	13

## TECHNICAL EXHIBIT 2 Information Assurance

	An Illegal Logon Tracked.	0	252	252	360	360	360	3325	3112	3156	72	96	96	52	52	52	484	760	760
	IA Annual Training.																0	0	0
<b>C.5.4.3.</b>	<b>Certification and Accreditation</b>																		
	A DITSCAP Approved. Unclass	0	1	1				1	1	1	2	2	2	1	1	1	3	4	4
	A DITSCAP Approved. Class	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1	3	3	3
	A Reaccreditation Approved Unclass	0	0	0	0	0	0	1	1	1	0	0	1	1	1	1	1	1	2
	A Reaccreditation Approved Class	0	0	0	1	1	1	1	1	1	0	0	1	1	1	1	2	2	3
	An IA Security Tool is Planned and Purchased.	1	1	2	1	1	1	2	2	2	1	2	2	1	1	1	4	5	6
<b>C.5.4.4.</b>	<b>Provide DoD PKI Support</b>																		
	A DoD PKI Supported	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	A Common Access Card Authentication Supported.	28	33	80	5	20	7	0	0	96	0	150	200	0	0	0	33	203	287
	A Common Access Card device supported. Work Station	1	1	1	1	1	1	0	1	1	1	0	0	0	0	0	3	2	2
	A Common Access Card device supported. Mobile	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	1	1
	A Common Access Card device supported. Pin Reset	0	0	0	0	0	0	0	0	0	0	0	1	0	0	1	0	0	2
	A CEFMS signature card requested.	300	300	300	3	1	2	200	205	210	100	50	75	26	27	26	429	378	403
<b>C.5.4.5.</b>	<b>Perform COMSEC</b>																		
	A COMSEC Inspection Program is Established and Maintained.	1	1	2	0	0	0	2	1	2	1	0	2	0	0	0	2	1	4
	A Sub-Account or Hand Receipt Holder Reviewed. - Sub Account	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	A Sub-Account or Hand Receipt Holder Reviewed. - Hand Receipt	10	10	10	0	0	0	0	0	0	0	0	0	0	0	0	30	10	10
	A Key Vial, U.S. Flag Carrier or Foreign Commercial Aircraft Transported Outside the Continental U.S. Approved.	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	A Waiver to the Grade Restrictions for COMSEC is Submitted and Approved.	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	A Department of Army Cryptographic Access Program is Implemented and Monitored.		0	0		0	0	0	0	0		0	0		0	0	0	0	0
	A Department of Army Cryptographic Access Program Point of Contact Designated.	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	A Scheduled Report Provided.	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	A COMSEC Inspector, Custodian and Alternate are Appointed.	3	3	3	0	0	0	1	1	1	1	1	1	0	0	0	4	4	4
	A COMSEC Record is Created and Preserved.	0	0	0	0	0	0	72	66	72	0	0	0	0	0	0	0	0	0
	An Employee is Briefed, Certified or Terminated	6	6	6	0	0	0	3	3	3	4	4	4	0	0	0	10	10	10
	A Classified Material is Distributed and Maintained	2	2	2	0	0	0	1	1	2	3		3	3		3	8	2	8
	A Management Control Reviews Performed.	1	1	1	0	0	0	0	0	0	0	0	0	2	2	2	2	3	3
	An Electronic Key Required	8	8	8	0	0	0	16	16	16	70	70	70	36	36	36	114	114	114
	A Sub-Account Established	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	A COMSEC Risk Assessments Conducted.	2	2	2	0	0	0	1	1	1	1	1	1	0	0	0	3	3	3
	An Incident Reported	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	A COMSEC Employee Trained.	0	0	3	0	0	0	5	5	5	2	2	2	0	0	0	2	2	5
	An Incident Resolved	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

## TECHNICAL EXHIBIT 2 Information Assurance

<b>C.5.4.6.</b>	<b>Information Assurance Vulnerability Alert (IAVA) Reporting and Compliance (24/7 as required) including Bulletins (IAVB), Technical Tips (IAVTT) and Situational Awareness Reports (SARs)</b>																			
	An IAVA, IAVB, IATT, or SAR notice is coordinated and distributed.	51	82	56	51	82	56	51	82	56	51	82	56	51	82	56	204	328	224	
	An IAVA or IAVB is acknowledged.	28	54	72	28	54	72	28	54	72	28	54	72	28	54	72	112	216	288	
	An IAVA notice completed and reported to higher headquarters.	21	34	48	21	34	48	21	34	48	21	34	48	21	34	48	84	136	192	
	A required scan performed.	46	68	96	46	68	96	46	68	96	46	68	96	46	68	96	184	272	384	
	An IA software patch is applied or a configuration change is made and documented.	60	96	96	1500	1500	1500	10983	13944	15432	16000	19450	21000	6233	6233	6233	23793	27279	28829	
	Populate the Compliance Reporting Database (CRD2) and maintain to current IAVA compliance																0	0	0	
<b>C.5.4.7.</b>	<b>Monitor and Manage Network Security (24/7 as required)</b>																			
	A network scan completed	16	50	50	500	500	500	360	384	408	100	100	100	144	144	144	760	794	794	
	An anomaly reported	0	12	12	0	0	0	721	1087	540	0	0	0	0	0	0	0	12	12	
	A trend analysis conducted.	0	0	0	0	0	0	32	43	58	0	0	0	0	0	0	0	0	0	
	A Security Issue Coordinated	32	40	30	17	22	25	22	31	38	0	13	20	19	19	19	68	94	94	
	A Web-page is reviewed for personally identifying (or other inappropriate information)							7275	7390	7485				0	0	0	0	0	0	
	A Web-page is reviewed for conformance to the American Disabilities Act (ADA-Section 508 compliance)							7275	7390	7485				0	0	0	0	0	0	
	A Official or Local Policy Established	2	19	22	1	1	1	2	2	2	1	1	1	3	3	3	7	24	27	
	A Firewall system provided.	0	0	0	1	1	1	0	0	0	4	4	6	0	0	0	5	5	7	
Workload data in TE 2 GFE	An Antivirus Software system upgraded and updated.																			
	An IDS System Maintained.	0	0	0	1	1	1	0	0	0	0	0	0	0	0	0	1	1	1	
	A VPN Concentrator Installed	0	0	1	0	0	0	2	0	5	0	0	1	0	0	0	0	0	2	
	A Physical Restricted Area Policy Enforced.	1	1	1	48	48	48	2	2	2	1	1	1	3	3	3	53	53	53	
	A Physical Restricted Area Policy Enforced.	1	1	1	12	12	12	1	1	1	1	1	1	3	3	3	17	17	17	
	An enclave is established.	1	1	1	12	12	12	27	27	27	2	2	2	1	1	1	16	16	16	
	An enclave is established.	1	1	1	12	12	12	1	1	1	1	1	1	1	1	1	15	15	15	
	A Remote Access Server (RAS) Managed.	2	2	2	1	1	1	2	2	2	1	3	3	1	1	1	5	7	7	
	A Wireless Access Concentrator Maintained.	0	0	1	24	24	36	0	0	0	0	0	16	1	1	1	25	25	54	
	A wireless security review is conducted							0	1	3				0	0	0	0	0	0	
	An Internet Filtering Software System Maintained.	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
	An Intrusion Test Performed.	2	2	2	0	0	0	2	1	2	1	1	1	1	1	1	4	4	4	
	An Anti-Spam, Spyware and Adware System Maintained. Unclassified	0	1000	1200	0	0	0	192	192	192	0	0	0	0	0	0	0	1000	1200	
	An Anti-Spam, Spyware and Adware System Maintained. Classified																0	0	0	
<b>C.5.4.8.</b>	<b>Security Incidents</b>																			
	A Security Incident Reported.	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	1	0	
	An Incident Log History Provided.	0	10	5	0	0	0	4	4	4	1	1	1	0	0	0	1	11	6	
	A virus is found and removed.							532	592	610				0	0	0	0	0	0	

## TECHNICAL EXHIBIT 2 Information Assurance

	A Device Purged.	0	0	0	0	0	0	24	24	24	2	3	3	48	48	97	50	51	100
	An IA Incident Processed.	0	10	5	8	10	10	12	12	12	2	3	3	0	0	0	10	23	18
<b>C.5.4.9.</b>	<b>SA / IASO responsibilities</b>																		
	A Hard Drive Wiped.	350	350	350	145	160	136	90	82	82	12	12	12	4	4	4	511	526	502
	A New System Evaluated	350	350	350	0	0	0	25	25	340	150	200	200	0	0	0	500	550	550
<b>C.5.4.10.</b>	A System Backup Completed	7830	7830	7830	12	12	12	6370	6370	6370	9100	9100	1200	432	216	0	17374	17158	9042

**TECHNICAL EXHIBIT 2  
Information Assurance**

PARAGRAPH NUMBER	TITLE	CEHQ			CEEIS			CEHNC			CEFC (Millington)			CEFC (Huntsville)			CEERD			HQ, CENTERS, LABS TOTALS		
		FY03	FY04	FY05	FY03	FY04	FY05	FY03	FY04	FY05	FY03	FY04	FY05	FY03	FY04	FY05	FY03	FY04	FY05	FY03	FY04	FY05
<b>C.5.4</b>	<b>INFORMATION ASSURANCE</b>																					
<b>C.5.4.1</b>	<b>Manage Information Assurance Program</b>																					
	A Security Program Provided	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	3	3	3
	An IA Law, Policy, or Regulation Change Reviewed.	16	11	14	29	29	35	4	4	4	1	3	0	15	18	30	16	10	16	35	32	50
	An IA User-Training Program Provided	1248	1473	1551			170	697	410		296	385			763	2733	2310	2919	3430	3483	2919	
	IA Personnel Trained.	12	10	11	100	105	108	18	18	18	3	3	3	3	3	3	20	20	18	41	41	39
	An IA Appointment Letter Written and Maintained.	1	1	9	34	34	45	4	3	2	3	3	3	3	4	4	75	75	110	82	82	116
	An IA Memorandum of Agreement/Memorandum of Understanding (MOA/MOU) Maintained.	0	0	0	67	67	67	2	2	4	0	1	1	3	3	3	10	10	10	15	15	17
Workload data in TE 2 GFE	A Software License Maintained.															14761	14761	14761				
	An IA Report, Recommendation, or Briefing Completed or Meeting Held.	1009	1512	1512	360	350	350	134	122	134	12	12	12	2	2	2	300	400	520	436	524	656
	IA Information Disseminated.	102	112	100	70	75	80	60	68	80	4	4	4	0	0	0	76	53	76	136	121	156
	An IA Report Prepared	26	32	39	10	10	10	20	25	30	0	0	0	0	0	0	21	18	21	41	43	51
	A Risk Mitigation Recommended	36	43	47	75	80	85	5	3	6	0	0	0	0	0	0	11	10	11	16	13	17
	An IA Inquiry Resolved	360	432	400	7982	8100	8350	150	150	150	5	5	5	0	0	0	870	718	925	1020	868	1075
	IA Threats and Vulnerabilities Evaluated.	93	127	160	177	172	202	27	59	87	25	25	25		42	40	96	128	158	123	229	285
	A Security Audit, Inspection or Investigation Conducted	8	12	14	3	3	3	1	1	1	1	1	1	2	1	1	12	12	16	15	14	18
Workload data in TE 2 GFE	An audit trail, review, and archive is established and maintained.															470	473	528				
	An IA Issue Coordinated With Other Agencies.	1040	1040	1040	0	7200	7340				0	0	0	0	0	0	86	92	96	86	92	96
	An IA Issue Coordinated with COE program.	9360	14040	16000	600	500	400	12	12	12	3	3	3	0	0	0	15	14	15	27	26	27
	A Networkiness Certification Completed.	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	1	0	3	2	1	4
	A Budget is Executed and Managed.	2	2	2	1	1	2	6	6	6	1	1	1	1	1	1	1	1	1	8	8	8
	IA Procurements Reviewed.	4	4	4	2	6	6	4	5	3	0	0	0	1	1	1	12	26	35	17	32	39
	Participated on Configuration Management Board.	0	1	4	8	8	10	3	3	3	0	0	0	1	2	2	8	8	8	12	13	13
	An IA Inspection Conducted	3	0	12	236	236	250	12	24	30	48	48	48	2		1	8	7	7	22	31	38
<b>C.5.4.2.</b>	<b>Manage userIDs and passwords for all systems. Enforce system access, operation, maintenance and disposition in accordance with policies and practices.</b>																					
Workload data in TE 2 C.5.2.7.1	An Unclassified Account, Password, Permission, Inactivity or Suspension Policy Managed.																					
Workload data in TE 2 C.5.2.7.2	A Classified Account, Password, Permission, Inactivity or Suspension Policy Managed.																					
	An IA Personnel Security Clearance Verified.	0	0	0	105	107	108	16	17	17	3	3	3	40	60	0	71	66	62	127	143	79
	A default, guest or services accounts removed, changed or disabled.	3	2	0	158	183	190	268	268	301	9	5	0	1	1	1	4200	4350	4500	4469	4619	4802
	An Privileged Account Issued.	0	0	0	194	413	493	8	21	8	3	3	3	2	2	2	8500	9000	9500	8510	9023	9510
	A Password Reissued.	0	0	0	20	20	20	48	36	60	3	3	3	24	24	24	22	22	0	94	82	84
	Verification for INFOSEC Training Provided.	0	0	0	1	1	1	12	12	12	12	12	12	3	3	3	3	3	3	18	18	18
	A Password Compliance Tested	10	20	50	34560	34560	34560	0	12	12	0	0	0	3	3	3	2	2	2	5	17	17
	An Illegal Logon Tracked.	0	0	0	41760	41880	42920	1440	1440	1440	0	0	0	12	12	12	36500	32000	38000	37952	33452	39452
	IA Annual Training.				104	105	110												0	0	0	0
<b>C.5.4.3.</b>	<b>Certification and Accreditation</b>																					
	A DITSCAP Approved. Unclass	5	8	10	1	1	1	4	4	4	0	1	0	2	2	2	1	1	1	7	7	7
	A DITSCAP Approved. Class	0	1	2	1	1	1	0	2	3	0	0	0	0	0	0	5	3	4	5	5	7
	A Reaccreditation Approved Unclass	3	10	20	0	1	1	4	4	4	0	0	1	0	2	2	1	1	1	5	7	7
	A Reaccreditation Approved Class	0	0	1	0	1	1	0	2	2	0	0	1	0	0	0	5	5	5	5	7	7
	An IA Security Tool is Planned and Purchased.	2	3	6	0	0	7	1	2	3	0	1	1	0	2	2	9	17	18	10	21	23

**TECHNICAL EXHIBIT 2  
Information Assurance**

<b>C.5.4.4.</b>	<b>Provide DoD PKI Support</b>																				0	0	0
	A DoD PKI Supported	0	0	0	0	0	10000	0	0	0	0	0	0	0	0	0	320	260	380	320	260	380	
	A Common Access Card Authentication Supported.	0	0	0	130	380	340	650	24	650	0	0	250	0	0	60				650	24	710	
	A Common Access Card device supported. Work Sta	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	2	0	2	2	0	
	A Common Access Card device supported. Mobile	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	4	4	0	4	4	
	A Common Access Card device supported. Pin Rese	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	1	1	
	A CEFMS signature card requested.	0	0	0	3641	3798	3816	104	148	171	173	179	175	23	23	23	480	570	600	607	741	794	
<b>C.5.4.5.</b>	<b>Perform COMSEC</b>																						
	A COMSEC Inspection Program is Established and Maintained.	13	4	12	14	48	48	0	0	2	0	0	0	0	0	4	4	4	4	4	6		
	A Sub-Account or Hand Receipt Holder Reviewed. - Sub Account	0	0	0	2	6	12	0	0	0	0	0	0	0	0	0	0	0	0	0	0		
	A Sub-Account or Hand Receipt Holder Reviewed. - Hand Receipt	3	3	1	50	52	60	0	0	0	0	0	0	0	0	4	4	4	4	4	4		
	A Key Vial, U.S. Flag Carrier or Foreign Commercial Aircraft Transported Outside the Continental U.S. Approved.	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0		
	A Waiver to the Grade Restrictions for COMSEC is Submitted and Approved.	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0		
	A Department of Army Cryptographic Access Program is Implemented and Monitored.	5	5	5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0		
	A Department of Army Cryptographic Access Program Point of Contact Designated.	2	2	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0		
	A Scheduled Report Provided.	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0		
	A COMSEC Inspector, Custodian and Alternate are Appointed.	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0		
	A COMSEC Record is Created and Preserved.	24	21	24	24	24	24	0	0	0	0	0	0	0	0	6	6	6	6	6	6		
	An Employee is Briefed, Certified or Terminated	50	50	50	16	26	16	0	0	0	0	0	0	0	0	43	52	43	43	52	43		
	A Classified Material is Distributed and Maintained	13	13	13	0	3	3	0	1	1	0	0	0	0	0	2	2	2	2	3	3		
	A Management Control Reviews Performed.	13	3	12	36	36	36	0	0	0	0	0	0	0	0	0	0	0	0	0	0		
	An Electronic Key Required	0	0	0	150	948	950	7	12	12	0	0	0	0	0	12	12	12	19	24	24		
	A Sub-Account Established	0	0	0	0	0	0	7	7	7	0	0	0	0	0	0	0	0	7	7	7		
	A COMSEC Risk Assessments Conducted.	13	13	13	0	1	0	0	0	0	0	0	0	0	0	4	4	4	4	4	4		
	An Incident Reported	1	2	3	0	1	0	0	0	0	0	0	0	0	0	2	0	2	2	0	2		
	A COMSEC Employee Trained.	2	4	4	0	6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0		
	An Incident Resolved	3	1	2	0	1	0	0	0	0	0	0	0	0	0	2	0	2	2	0	2		
<b>C.5.4.6.</b>	<b>Information Assurance Vulnerability Alert (IAVA) Reporting and Compliance (24/7 as required) including Bulletins (IAVB), Technical Tips (IAVTT) and Situational Awareness Reports (SARs)</b>																						
	An IAVA, IAVB, IATT, or SAR notice is coordinated and distributed.	51	82	56	51	82	56	51	82	56	51	82	56	51	82	56	204	328	224	306	492	336	
	An IAVA or IAVB is acknowledged.	28	54	72	28	54	72	28	54	72	28	54	72	28	54	72	112	216	288	168	324	432	
	An IAVA notice completed and reported to higher headquarters.	21	34	48	21	34	48	21	34	48	21	34	48	21	34	48	84	136	192	126	204	288	
	A required scan performed.	46	68	96	46	68	96	46	68	96	46	68	96	46	68	96	184	272	384	276	408	576	
	An IA software patch is applied or a configuration change is made and documented.	51	82	108	10800	112861	122505	8100	8100	8100	1402	6512	6512		770	600	55200	61200	85600	63300	70070	94300	
	Populate the Compliance Reporting Database (CRD2) and maintain to current IAVA compliance				324	802	1000																
<b>C.5.4.7.</b>	<b>Monitor and Manage Network Security (24/7 as required)</b>																						
	A network scan completed	21	28	84	35	35	44		137		60	60	60	0	0	0	697	811	950	697	948	950	
	An anomaly reported				600	600	800	12	12	12	0	0	0	0	0	0	850	1090	1275	862	1102	1287	
	A trend analysis conducted.		33		8680	10160	13440	0	0	0	0	0	0	0	0	84	62	84	84	62	84		

**TECHNICAL EXHIBIT 2  
Information Assurance**

	A Security Issue Coordinated	12	12	12	6	6	7	48	48	48	0	0	0	0	0	0	138	170	225	186	218	273
	A Web-page is reviewed for personally identifying (or other inappropriate information)				0	159	159				3633	4353	4400	0	0	0	39000	38200	35000	39000	38200	35000
	A Web-page is reviewed for conformance to the American Disabilities Act (ADA-Section 508 compliance)				0	54	54				3633	4353	4400	0	0	0	39000	38200	35000	39000	38200	35000
	A Official or Local Policy Established	8	14	12	9	9	9	14	14	14	358	358	358	0	0	0	17	23	29	31	37	43
	A Firewall system provided.	0	0	0	60	144	150	0	0	0	0	0	0	0	0	0	6	10	11	6	10	11
Workload data in TE 2 GFE	An Antivirus Software system upgraded and updated.																4250	4350	4500			
	An IDS System Maintained.	0	0	0	80	80	160	0	0	0	0	0	0	0	0	0	4	7	8	4	7	8
	A VPN Concentrator Installed	0	0	0	5	15	20	0	0	0	0	0	0	0	0	0	10	19	21	10	19	21
	A Physical Restricted Area Policy Enforced.	0	0	0	5	5	5	1	1	1	4	4	4	2	2	2	5	5	5	8	8	8
	A Physical Restricted Area Policy Enforced.	0	0	0	2	2	2	1	1	1	0	0	0	0	0	0	3	3	3	4	4	4
	An enclave is established.	0	0	0	82	121	152	6	5	5	1	1	1	0	0	0	18	18	19	24	23	24
	An enclave is established.	0	0	0	2	2	2	0	1	1	0	0	0	0	0	0	10	10	13	10	11	14
	A Remote Access Server (RAS) Managed.	0	0	0	5	5	5	1	1	1	0	0	0	0	0	0	9	8	8	10	9	9
	A Wireless Access Concentrator Maintained.	0	0	0	0	3	7	0	0	0	0	0	0	0	0	0	10	117	155	10	117	155
	A wireless security review is conducted				15	15	15				0	0	0	0	0	0	9	10	16	9	10	16
	An Internet Filtering Software System Maintained.	0	0	0	0	0	2	0	0	0	0	0	0	0	0	0	23	27	28	23	27	28
	An Intrusion Test Performed.	8	45	100	126	126	135	0	0	0	0	1	0	2	2	2	9	9	9	11	11	11
	An Anti-Spam, Spyware and Adware System Maintained. Unclassified	0	0	0	23	23	25	0	12	24	0	0	0	2	2	2	0	2875	25229	2	2889	25255
	An Anti-Spam, Spyware and Adware System Maintained. Classified	0	0	0	2	2	2							0	0	0				0	0	0
<b>C.5.4.8.</b>	<b>Security Incidents</b>																					
	A Security Incident Reported.	41	48	48	0	0	0	3	0	1	0	0	0	0	0	0	35	28	35	38	28	36
	An Incident Log History Provided.	0	0	0	0	0	0	3	4	6	0	0	0	0	0	0	16	15	16	19	19	22
	A virus is found and removed.				1	0	1				0	0	0	5	5	5	20	5	3	25	10	8
	A Device Purged.	0	0	0	1	0	1	3	3	6	0	0	0	0	0	0	15	12	14	18	15	20
	An IA Incident Processed.	0	0	0	1	0	1	4	4	6	0	0	0	0	0	0	35	28	36	39	32	42
<b>C.5.4.9.</b>	<b>SA / IASO responsibilities</b>																					
	A Hard Drive Wiped.	0	0	0	10244	10567	748	326	294	300	126	30	75	0	27	4	120	95	120	446	416	424
	A New System Evaluated	0	0	0	55	54	74	156	147	168	1	4	2	0	27	4	640	693	673	796	867	845
<b>C.5.4.10.</b>	<b>A System Backup Completed</b>	0	0	0	119760	238120	297946	10332	12600	12600	2640	2640	2640	360	360	360	105	120	140	10797	13080	13100

## TECHNICAL EXHIBIT 2 Information Assurance

PARAGRAPH NUMBER	TITLE	CEHECSA			CEIWR (HEC)			CEIWR (NCR)			FOA TOTALS		
		FY03	FY04	FY05	FY03	FY04	FY05	FY03	FY04	FY05	FY03	FY04	FY05
<b>C.5.4</b>	<b>INFORMATION ASSURANCE</b>												
<b>C.5.4.1</b>	<b>Manage Information Assurance Program</b>												
	A Security Program Provided	1	1	1	1	1	1	1	1	1	3	3	3
	An IA Law, Policy, or Regulation Change Reviewed.				0	20	20				0	20	20
	An IA User-Training Program Provided	1412	1412	1412	62		98	95	203	126	1569	1615	1636
	IA Personnel Trained.	56	59	59	1	2	3	0	1	0	57	62	62
	An IA Appointment Letter Written and Maintained.	56	59	59	1	2	3	0	1	0	57	62	62
	An IA Memorandum of Agreement/Memorandum of Understanding (MOA/MOU) Maintained.	56	59	59	0	2	3	0	2	0	56	63	62
Workload data in TE 2 GFE	A Software License Maintained.												
	An IA Report, Recommendation, or Briefing Completed or Meeting Held.	140	172	205	0	2	2	0	10	0	140	184	207
	IA Information Disseminated.				16	16	16	0	0	0	16	16	16
	An IA Report Prepared	188	220	250	4	4	4	0	0	0	192	224	254
	A Risk Mitigation Recommended				4	4	4	0	0	0	4	4	4
	An IA Inquiry Resolved	140	172	200	24	24	24	0	0	0	164	196	224
	IA Threats and Vulnerabilities Evaluated.	32	37	42	100	100	100	0	0	0	132	137	142
	A Security Audit, Inspection or Investigation Conducted	1	1	1	0	2	2	0	0	0	1	3	3
Workload data in TE 2 GFE	An audit trail, review, and archive is established and maintained.												
	An IA Issue Coordinated With Other Agencies.										0	0	0
	An IA Issue Coordinated with COE program.				4	4	4	0	0	0	4	4	4
	A Networthiness Certification Completed.	1	1	1	0	1	1	0	0	7	1	2	9
	A Budget is Executed and Managed.				1	1	1	0	0	0	1	1	1
	IA Procurements Reviewed.	760	764	800	1	1	1	0	0	0	761	765	801
	Participated on Configuration Management Board.	0	0	0	1	1	1	0	0	0	1	1	1
	An IA Inspection Conducted	24	36	48	48	48	48	0	0	0	72	84	96
<b>C.5.4.2.</b>	<b>Manage userIDs and passwords for all systems. Enforce system access, operation, maintenance and disposition in accordance with policies and practices.</b>												
Workload data in TE 2 C.5.2.7.1	An Unclassified Account, Password, Permission, Inactivity or Suspension Policy Managed.												
Workload data in TE 2 C.5.2.7.2	A Classified Account, Password, Permission, Inactivity or Suspension Policy Managed.												
	An IA Personnel Security Clearance Verified.	57	60	60	6	6	6	0	0	0	63	66	66
	A default, guest or services accounts removed, changed or disabled.				60	60	60	0	0	0	120	120	120

## TECHNICAL EXHIBIT 2 Information Assurance

	An Privileged Account Issued.	56	59	59	5	5	5	0	0	0	61	64	64
	A Password Reissued.	36	865	506	12	12	12	0	0	0	48	877	518
	Verification for INFOSEC Training Provided.	4	8	8	0	5	5	0	0	0	4	13	13
	A Password Compliance Tested	12	20	36	0	0	1	0	0	0	12	20	37
	An Illegal Logon Tracked.		250	420	0	0	48	0	0	0	0	250	468
	IA Annual Training.										0	0	0
<b>C.5.4.3.</b>	<b>Certification and Accreditation</b>												
	A DITSCAP Approved. Unclass	0	2	2	0	1	0	0	0	0	0	3	2
	A DITSCAP Approved. Class	0	1	2	0	0	0	0	0	0	0	1	2
	A Reaccreditation Approved Unclass	0	2	2	0	0	0	0	0	0	0	2	2
	A Reaccreditation Approved Class	0	2	2	0	0	0	0	0	0	0	2	2
	An IA Security Tool is Planned and Purchased.				0	0	1	0	0	0	0	0	1
<b>C.5.4.4.</b>	<b>Provide DoD PKI Support</b>												
	A DoD PKI Supported	0	0	0	0	0	0	0	0	0	0	0	0
	A Common Access Card Authentication Supported.				0	8	12	0	0	0	0	8	12
	A Common Access Card device supported. Work Stat	0	2	2	0	0	0	0	0	0	0	2	2
	A Common Access Card device supported. Mobile	0	0	0	0	0	0	0	0	0	0	0	0
	A Common Access Card device supported. Pin Reset	0	2	2	0	0	0	0	0	0	0	2	2
	A CEFMS signature card requested.	620	25	620	6	6	6				626	31	626
<b>C.5.4.5.</b>	<b>Perform COMSEC</b>												
	A COMSEC Inspection Program is Established and Maintained.	1	1	1	0	0	0	0	0	0	1	1	1
	A Sub-Account or Hand Receipt Holder Reviewed. - Sub Account	0	0	0	0	0	0	0	0	0	0	0	0
	A Sub-Account or Hand Receipt Holder Reviewed. - Hand Receipt	10	10	10	0	0	0	0	0	0	10	10	10
	A Key Vial, U.S. Flag Carrier or Foreign Commercial Aircraft Transported Outside the Continental U.S. Approved.	0	0	0	0	0	0	0	0	0	0	0	0
	A Waiver to the Grade Restrictions for COMSEC is Submitted and Approved.	0	0	0	0	0	0	0	0	0	0	0	0
	A Department of Army Cryptographic Access Program is Implemented and Monitored.	1	1	1	0	0	0	0	0	0	1	1	1
	A Department of Army Cryptographic Access Program Point of Contact Designated.	1	1	1	0	0	0	0	0	0	1	1	1
	A Scheduled Report Provided.	0	0	0	0	0	0	0	0	0	0	0	0
	A COMSEC Inspector, Custodian and Alternate are Appointed.	1	1	1	0	0	0	0	0	0	1	1	1
	A COMSEC Record is Created and Preserved.	12	12	12	0	0	0	0	0	0	12	12	12
	An Employee is Briefed, Certified or Terminated	0	0	0	0	0	0	0	0	0	0	0	0
	A Classified Material is Distributed and Maintained				0	0	0	0	0	0	0	0	0
	A Management Control Reviews Performed.				0	0	0	0	0	0	0	0	0
	An Electronic Key Required	60	50	60	0	0	0	0	0	0	60	50	60

## TECHNICAL EXHIBIT 2 Information Assurance

	A Sub-Account Established	0	0	0	0	0	0	0	0	0	0	0	0
	A COMSEC Risk Assessments Conducted.	2	2	0	0	0	0	0	0	0	2	2	0
	An Incident Reported	0	0	0	0	0	0	0	0	0	0	0	0
	A COMSEC Employee Trained.	0	1	2	0	0	0	0	0	0	0	1	2
	An Incident Resolved	0	0	0	0	0	0	0	0	0	0	0	0
<b>C.5.4.6.</b>	<b>Information Assurance Vulnerability Alert (IAVA) Reporting and Compliance (24/7 as required) including Bulletins (IAVB), Technical Tips (IAVTT) and Situational Awareness Reports (SARs)</b>												
	An IAVA, IAVB, IATT, or SAR notice is coordinated and distributed.	51	82	56	51	82	56	51	82	56	153	246	168
	An IAVA or IAVB is acknowledged.	28	54	72	28	54	72	28	54	72	84	162	216
	An IAVA notice completed and reported to higher headquarters.	21	34	48	21	34	48	21	34	48	63	102	144
	A required scan performed.	46	68	96	46	68	96	46	68	96	138	204	288
	An IA software patch is applied or a configuration change is made and documented.	88	120	144	96	96	96	0	0	0	184	216	240
	Populate the Compliance Reporting Database (CRD2) and maintain to current IAVA compliance												
<b>C.5.4.7.</b>	<b>Monitor and Manage Network Security (24/7 as required)</b>												
	A network scan completed	3	3	3	48	48	48	0	0	0	51	51	51
	An anomaly reported	0	0	0	2	2	2	0	0	0	2	2	2
	A trend analysis conducted.		36	36	2	2	2	0	0	0	2	38	38
	A Security Issue Coordinated	21			2	2	2	0	0	0	23	2	2
	A Web-page is reviewed for personally identifying (or other inappropriate information)	67144	67144	10071							67144	67144	10071
	A Web-page is reviewed for conformance to the American Disabilities Act (ADA-Section 508 compliance)	74632	74632	11195							74632	74632	11195
	A Official or Local Policy Established		5		2	4	8	0	0	0	2	9	8
	A Firewall system provided.				1	1	1	0	0	0	1	1	1
Workload data in TE-2 GFE	An Antivirus Software system upgraded and updated.												
	An IDS System Maintained.				1	1	1	0	0	0	1	1	1
	A VPN Concentrator Installed				0	0	0	0	0	0	0	0	0
	A Physical Restricted Area Policy Enforced.	2	2	2	1	1	1	0	0	0	3	3	3
	A Physical Restricted Area Policy Enforced.	2	2	2	0	0	0	0	0	0	2	2	2
	An enclave is established.	2	2	2	1	1	1	0	0	0	3	3	3
	An enclave is established.	1	1	1	0	0	0	0	0	0	1	1	1
	A Remote Access Server (RAS) Managed.		2		0	0	0	0	0	0	0	2	0
	A Wireless Access Concentrator Maintained.				0	0	0	0	0	0	0	0	0
	A wireless security review is conducted	2	0	2							2	0	2
	An Internet Filtering Software System Maintained.				0	0	0	0	0	0	0	0	0

## TECHNICAL EXHIBIT 2 Information Assurance

	An Intrusion Test Performed.		2		0	1	2	0	0	0	0	3	2
	An Anti-Spam, Spyware and Adware System Maintained. Unclassified				0	0	1	0	0	0	0	0	1
	An Anti-Spam, Spyware and Adware System Maintained. Classified							0	0	0	0	0	0
<b>C.5.4.8.</b>	<b>Security Incidents</b>												
	A Security Incident Reported.	2	0	1	0	0	0	0	0	0	2	0	1
	An Incident Log History Provided.				0	0	1	0	0	0	0	0	1
	A virus is found and removed.	41	30	0							41	30	0
	A Device Purged.	0	0		0	0	0	0	0	0	0	0	0
	An IA Incident Processed.				1	1	1	0	0	0	1	1	1
<b>C.5.4.9.</b>	<b>SA / IASO responsibilities</b>												
	A Hard Drive Wiped.	265	227	240	20	20	20	0	0	0	285	247	260
	A New System Evaluated		450		20	20	20	0	0	0	20	470	20
<b>C.5.4.10.</b>	A System Backup Completed	960	960	960	600	600	600	0	0	0	1560	1560	1560

## TECHNICAL EXHIBIT 2 Information Assurance

PARAGRAPH NUMBER	TITLE	ITIPS			OMBIL			AIS TOTALS		
		FY03	FY04	FY05	FY03	FY04	FY05	FY03	FY04	FY05
<b>C.5.4</b>	<b>INFORMATION ASSURANCE</b>							0	0	0
<b>C.5.4.1</b>	<b>Manage Information Assurance Program</b>							0	0	0
	A Security Program Provided							0	0	0
	An IA Law, Policy, or Regulation Change Reviewed.							0	0	0
	An IA User-Training Program Provided							0	0	0
	IA Personnel Trained.				0	1	0	0	1	0
	An IA Appointment Letter Written and Maintained.				0	1	0	0	1	0
	An IA Memorandum of Agreement/Memorandum of Understanding (MOA/MOU) Maintained.				0	5	0	0	5	0
Workload data in TE-2 GFE	A Software License Maintained.									
	An IA Report, Recommendation, or Briefing Completed or Meeting Held.							0	0	0
	IA Information Disseminated.							0	0	0
	An IA Report Prepared							0	0	0
	A Risk Mitigation Recommended							0	0	0
	An IA Inquiry Resolved							0	0	0
	IA Threats and Vulnerabilities Evaluated.							0	0	0
	A Security Audit, Inspection or Investigation Conducted							0	0	0
Workload data in TE-2 GFE	An audit trail, review, and archive is established and maintained.									
	An IA Issue Coordinated With Other Agencies.				0	0	0	0	0	0
	An IA Issue Coordinated with COE program.				0	0	0	0	0	0
	A Networkiness Certification Completed.	1	1	1				1	1	1
	A Budget is Executed and Managed.							0	0	0
	IA Procurements Reviewed.	1	1	1	1	1	1	2	2	2
	Participated on Configuration Management Board.							0	0	0
	An IA Inspection Conducted				0	0	0	0	0	0
<b>C.5.4.2.</b>	<b>Manage userIDs and passwords for all systems. Enforce system access, operation, maintenance and disposition in accordance with policies and practices.</b>									
Workload data in TE-2 C.5.2.7.1	An Unclassified Account, Password, Permission, Inactivity or Suspension Policy Managed.									
Workload data in TE-2 C.5.2.7.2	A Classified Account, Password, Permission, Inactivity or Suspension Policy Managed.									
	An IA Personnel Security Clearance Verified.				0	0	0	0	0	0

## TECHNICAL EXHIBIT 2 Information Assurance

	A default, guest or services accounts removed, changed or disabled.						0	0	0
	An Privileged Account Issued.			0	0	0	0	0	0
	A Password Reissued.						0	0	0
	Verification for INFOSEC Training Provided.			0	0	0	0	0	0
	A Password Compliance Tested			0	10	0	0	10	0
	An Illegal Logon Tracked.			0	0	0	0	0	0
	IA Annual Training.						0	0	0
<b>C.5.4.3.</b>	<b>Certification and Accreditation</b>								
	A DITSCAP Approved. Unclass						0	0	0
	A DITSCAP Approved. Class						0	0	0
	A Reaccreditation Approved Unclass						0	0	0
	A Reaccreditation Approved Class						0	0	0
	An IA Security Tool is Planned and Purchased.						0	0	0
<b>C.5.4.4.</b>	<b>Provide DoD PKI Support</b>								
	A DoD PKI Supported			0	0	0	0	0	0
	A Common Access Card Authentication Supported.			0	0	0	0	0	0
	A Common Access Card device supported. Work Station						0	0	0
	A Common Access Card device supported. Mobile						0	0	0
	A Common Access Card device supported. Pin Reset						0	0	0
	A CEFMS signature card requested.						0	0	0
<b>C.5.4.5.</b>	<b>Perform COMSEC</b>								
	A COMSEC Inspection Program is Established and Maintained.			0	0	0	0	0	0
	A Sub-Account or Hand Receipt Holder Reviewed. - Sub Account			0	0	0	0	0	0
	A Sub-Account or Hand Receipt Holder Reviewed. - Hand Receipt						0	0	0
	A Key Vial, U.S. Flag Carrier or Foreign Commercial Aircraft Transported Outside the Continental U.S. Approved.			0	0	0	0	0	0
	A Waiver to the Grade Restrictions for COMSEC is Submitted and Approved.			0	0	0	0	0	0
	A Department of Army Cryptographic Access Program is Implemented and Monitored.				0	0	0	0	0
	A Department of Army Cryptographic Access Program Point of Contact Designated.			0	0	0	0	0	0
	A Scheduled Report Provided.			0	0	0	0	0	0
	A COMSEC Inspector, Custodian and Alternate are Appointed.			0	0	0	0	0	0
	A COMSEC Record is Created and Preserved.			0	0	0	0	0	0
	An Employee is Briefed, Certified or Terminated			0	0	0	0	0	0
	A Classified Material is Distributed and Maintained			0		0	0	0	0
	A Management Control Reviews Performed.			0	0	0	0	0	0

## TECHNICAL EXHIBIT 2 Information Assurance

	An Electronic Key Required				0	0	0	0	0	0
	A Sub-Account Established				0	0	0	0	0	0
	A COMSEC Risk Assessments Conducted.				0	0	0	0	0	0
	An Incident Reported				0	0	0	0	0	0
	A COMSEC Employee Trained.				0	0	0	0	0	0
	An Incident Resolved				0	0	0	0	0	0
<b>C.5.4.6.</b>	<b>Information Assurance Vulnerability Alert (IAVA) Reporting and Compliance (24/7 as required) including Bulletins (IABV), Technical Tips (IAVTT) and Situational Awareness Reports (SARs)</b>									
	An IAVA, IAVB, IATT, or SAR notice is coordinated and distributed.	0	0	0	0	0	0	0	0	0
	An IAVA or IAVB is acknowledged.	0	0	0	0	0	0	0	0	0
	An IAVA notice completed and reported to higher headquarters.	0	0	0	0	0	0	0	0	0
	A required scan performed.	0	0	0	0	0	0	0	0	0
	An IA software patch is applied or a configuration change is made and documented.				0	0	0	0	0	0
	Populate the Compliance Reporting Database (CRD2) and maintain to current IAVA compliance							0	0	0
<b>C.5.4.7.</b>	<b>Monitor and Manage Network Security (24/7 as required)</b>									
	A network scan completed				0	0	0	0	0	0
	An anomaly reported				0	0	0	0	0	0
	A trend analysis conducted.				0	0	0	0	0	0
	A Security Issue Coordinated							0	0	0
	A Web-page is reviewed for personally identifying (or other inappropriate information)							0	0	0
	A Web-page is reviewed for conformance to the American Disabilities Act (ADA-Section 508 compliance)							0	0	0
	A Official or Local Policy Established				0	0	0	0	0	0
	A Firewall system provided.				0	0	0	0	0	0
Workload data in TE-2 GFE	An Antivirus Software system upgraded and updated.									
	An IDS System Maintained.				0	0	0	0	0	0
	A VPN Concentrator Installed				0	0	0	0	0	0
	A Physical Restricted Area Policy Enforced.				0	0	0	0	0	0
	A Physical Restricted Area Policy Enforced.							0	0	0
	An enclave is established.							0	0	0
	An enclave is established.							0	0	0
	A Remote Access Server (RAS) Managed.							0	0	0
	A Wireless Access Concentrator Maintained.				0	0	0	0	0	0
	A wireless security review is conducted							0	0	0
	An Internet Filtering Software System Maintained.				0	0	0	0	0	0

## TECHNICAL EXHIBIT 2 Information Assurance

	An Intrusion Test Performed.				0	0	0	0	0	0
	An Anti-Spam, Spyware and Adware System Maintained. Unclassified				0	0	0	0	0	0
	An Anti-Spam, Spyware and Adware System Maintained. Classified							0	0	0
<b>C.5.4.8.</b>	<b>Security Incidents</b>									
	A Security Incident Reported.				0	0	0	0	0	0
	An Incident Log History Provided.				0	0	0	0	0	0
	A virus is found and removed.							0	0	0
	A Device Purged.							0	0	0
	An IA Incident Processed.				0	0	0	0	0	0
<b>C.5.4.9.</b>	<b>SA / IASO responsibilities</b>									
	A Hard Drive Wiped.				0	0	0	0	0	0
	A New System Evaluated	0	1	0	0	0	0	0	1	0
<b>C.5.4.10.</b>	A System Backup Completed				0	0	0	0	0	0