FISMA				
2006 Scoring Methodology				
Report Grading Element				**FY06 Possible Points**
				100
A. Annual Testing				**20**
1	**The percentage of the agency's systems reviewed, including contractor systems, in FY06 was:**			**20**
	i)	**The percentage of agency systems reviewed in FY06 was:**		**10**
		HIGH Impact Systems		**6**
		a	Between 90 and 100%	6
		b	Between 75 and 89%	4
		c	Between 60 and 74%	2
		d	Between 45 and 59%	0.5
		e	44% and less	0
		Moderate Impact Systems		**3**
		a	Between 90 and 100%	3
		b	Between 75 and 89%	2
		c	Between 60 and 74%	1
		d	Between 45 and 59%	0.5
		e	44% and less	0
		Low Impact Systems		**1**
		a	Between 96 and 100%	1
		b	Between 51and 95%	0.5
		c	50% and less	0
		The percentage of contractor systems reviewed in FY06 was:		**10**
		HIGH Impact Systems		**6**
		a	Between 90 and 100%	6
		b	Between 75 and 89%	4
		c	Between 60 and 74%	2
		d	Between 45 and 59%	0.5

	ii)	e	44% and less	0
		Moderate Impact Systems		**3**
		a	Between 90 and 100%	3
		b	Between 75 and 89%	2
		c	Between 60 and 74%	1
		d	Between 45 and 59%	0.5
		e	44% and less	0
		Low Impact Systems		**1**
		a	Between 96 and 100%	1
		b	Between 51and 95%	0.5
		c	50% and less	0
	iii)	**The agency performs oversight and evaluation to ensure information systems used or operated by a contractor of the agency or other organization on behalf of the agency meet the requirements of FISMA, OMB policy and NIST guidelines, national security policy, and agency policy. (Self-reporting of NIST Special Publication 800-26 requirements by a contractor or other organization is not sufficient, however, self-reporting by another Federal agency may be sufficient.)**		**0**
		OIG Evaluation		
		a	Between 96 and 100%	0%
		b	Between 51and 95% (Loss of 1/2 Annual Testing points in A.1)	-50%
		c	50% and less (Loss of all Annual Testing points in A.1)	-100%
B. Plan of Action and Milestones (POA&M)				**15**
2	**Has the agency developed, implemented, and managing an agency-wide plan of action and milestone process? (OIG Assessment)**			**15**
	i)	**The POA&M is an agency wide process, incorporating all known IT security weaknesses associated with information systems used or operated by the agency or by a contractor of the agency or other organization on behalf of the agency.**		**3**
		a	Between 96 and 100%	3

		b	Between 81and 95%	2
		c	Between 71 and 80%	1
		d	Between 51and 70%	0.5
		e	50% and less	0
	ii)	**When an IT security weakness is identified, program officials (including CIOs, if they own or operate a system) develop, implement, and manage POA&Ms for their system(s).**		**4**
		a	Between 96 and 100%	4
		b	Between 81and 95%	2
		c	Between 71 and 80%	1
		d	Between 51and 70%	0.5
		e	50% and less	0
	iii)	**Program officials, including contractors, report to the CIO on a regular basis (at least quarterly) on their remediation progress.**		**1**
		a	Between 96 and 100%	1
		b	Between 51and 95%	0.5
		c	50% and less	0
	iv)	**CIO centrally tracks, maintains, and reviews POA&M activities on at least a quarterly basis.**		**2**
		a	Between 96 and 100%	2
		b	Between 81and 95%	1.5
		c	Between 71 and 80%	1
		d	Between 51and 70%	0.5
		e	50% and less	0
	v)	**OIG findings are incorporated into the POA&M process.**		**2**
		a	Between 96 and 100%	2
		b	Between 51and 95%	1
		c	50% and less	0
		POA&M process prioritizes IT security weaknesses to help ensure significant IT security weaknesses are addressed in a timely manner and receive appropriate resources.		**3**

	vi)	a	Between 96 and 100%	3
		b	Between 81and 95%	2
		c	Between 71 and 80%	1
		d	Between 51and 70%	0.5
		e	50% and less	0
C. Certification and Accreditation (C&A)				**20**
3	i)	**The percentage of systems that have been certified and accredited is:**		**12**
		HIGH Impact Systems		**6**
		a	Between 90 and 100%	6
		b	Between 75 and 89%	4
		c	Between 60 and 74%	3
		d	Between 45 and 59%	1
		e	44% and less	0
		Moderate Impact Systems		**4**
		a	Between 90 and 100%	4
		b	Between 75 and 89%	2
		c	Between 60 and 74%	1
		d	Between 45 and 59%	0.5
		e	44% and less	0
		Low Impact Systems		**2**
		a	Between 90 and 100%	2
		b	Between 75 and 89%	1.5
		c	Between 60 and 74%	1
		d	Between 45 and 59%	0.5
		e	44% and less	0
	ii)	**The percentage of systems whose security controls have been tested and evaluated in the last year is:**		**4**
		HIGH Impact Systems		**2**
		a	Between 90 and 100%	2
		b	Between 75 and 89%	1.5
		c	Between 60 and 74%	1
		d	Between 45 and 59%	0.5
		e	44% and less	0
		Moderate Impact Systems		**1.5**
		a	Between 96 and 100%	1.5

		b	Between 51and 95%	0.5
		c	50% and less	0
		Low Impact Systems		**0.5**
		a	Between 96 and 100%	0.5
		b	95% and less	0
	iii)	**The percentage of systems that have a contingency plan that has been tested in the past year:**		**4**
		HIGH Impact Systems		**2**
		a	Between 90 and 100%	2
		b	Between 75 and 89%	1.5
		c	Between 60 and 74%	1
		d	Between 45 and 59%	0.5
		e	44% and less	0
		Moderate Impact Systems		**1.5**
		a	Between 96 and 100%	1.5
		b	Between 51and 95%	0.5
		c	50% and less	0
		Low Impact Systems		**0.5**
		a	Between 51and 100%	0.5
		b	50% and less	0
	iv)	**OIG Assessment of the Certification and Accreditation Process**		**0**
		OIG C&A Evaluation		
		a	Excellent, Good, Satisfactory (No Deduction from C&A score in question 6i)	0%
		b	Poor (-1/2 of C&A points awarded in question 3i)	-50%
		c	Failing (-100% of C&A Points awarded in question 3i)	-100%
D. Configuration Management				**20**
4		**Is there an agency wide security configuration policy?**		**20**
		a	Yes	20
		b	No (Go to Section E, Question 7.i)	0
		Questions 1 through 11 only apply, if the agency has addressed the		
		1. Windows XP Professional		**0**
		a	Between 81 and 100% or (N/A)	0

		b	Between 71 and 80%	-0.5
		c	70% and less or (No)	-1
		2. Windows NT		**0**
		a	Between 81 and 100% or (N/A)	0
		b	Between 71 and 80%	-0.5
		c	70% and less or (No)	-1
		3. Windows 2000 Professional		**0**
		a	Between 81 and 100% or (N/A)	0
		b	Between 71 and 80%	-0.5
		c	70% and less or (No)	-1
		4. Windows 2000 Server		**0**
		a	Between 81 and 100% or (N/A)	0
		b	Between 71 and 80%	-0.5
		c	70% and less or (No)	-1
		5. Windows 2003 Server		**0**
		a	Between 81 and 100% or (N/A)	0
		b	Between 71 and 80%	-0.5
		c	70% and less or (No)	-1
	i)	**6. Solaris**		**0**
		a	Between 81 and 100% or (N/A)	0
		b	Between 71 and 80%	-0.5
		c	70% and less or (No)	-1
		7. HP-UX		**0**
		a	Between 81 and 100% or (N/A)	0
		b	Between 71 and 80%	-0.5
		c	70% and less or (No)	-1

		8. Linux		0
		a	Between 81 and 100% or (N/A)	0
		b	Between 71 and 80%	-0.5
		c	70% and less or (No)	-1
		9. Cisco Router IOS		0
		a	Between 81 and 100% or (N/A)	0
		b	Between 71 and 80%	-0.5
		c	70% and less or (No)	-1
		10. Oracle		0
		a	Between 81 and 100% or (N/A)	0
		b	Between 71 and 80%	-0.5
		c	70% and less or (No)	-1
		11. Other. Specify:		0
		a	Between 81 and 100% or (N/A)	0
		b	Between 71 and 80%	-0.5
		c	70% and less or (No)	-1
	ii)	Has the agency documented in its security policies special procedures for using emerging technologies (including but not limited to wireless and IPv6) and countering emerging threats (including but not limited to spyware, malware, etc.)?		
		a	Yes (No deductions)	0
		b	No (Loss of 4 points)	-4
E. Incident Detection and Response				**15**
5	i)	The agency follows documented policies and procedures for identifying and reporting incidents internally.		7
		a	Yes	7
		b	No	0

	ii)	The agency follows documented policies and procedures for external reporting to law enforcement authorities.		4
		a	Yes	4
		b	No	0
	iii)	The agency follows defined procedures for reporting to the United States Computer Emergency Readiness Team (US-CERT).		4
		a	Yes	4
		b	No	0
F. Training				**10**
6	Has the agency ensured security training and awareness of all employees, including contractors and those employees with significant IT Security responsibilities.			10
	i)	The percentage of agency employees (including contractors) that received IT security training and awareness as described in NIST SP 800-50 is:		4
		a	Between 96 and 100%	4
		b	Between 81 and 95%	3
		c	Between 71 and 80%	2
		d	Between 51 and 70%	1
		e	50% and less	0
	ii)	The percentage of employees with significant security responsibilities that received specialized security training as described in NIST SP 800-16 is:		4
		a	Between 96 and 100%	4
		b	Between 81 and 95%	3
		c	Between 71 and 80%	2
		d	Between 51 and 70%	1
		e	50% and less	0
	iii)	The agency provided the total training costs for FY06.		1
		a	Yes	1
		b	No	0

	iv)	**The agency explains policies regarding peer-to-peer file sharing in IT security awareness training, ethics training or any other agency-wide training.**		**1**
		a	Yes	**1**
		b	No	**0**
G. Inventory (No deductions or -10 maximum)				**0**
7	**What progress has the agency made to develop an inventory of major IT systems. (Must have no deductions for 10i, 10ii, 10iii or lose 10 pts)**			**0**
	i)	**The agency has developed an inventory of major information systems (including major national security systems) operated by or under the control of such agency, including an identification of the interfaces between each such system and all other systems or networks, including those not operated by or under the control of the agency. (IG evaluation)**		**0**
		a	Between 96 and 100%	0
		b	95% and less (Or the agency has no inventory)	-10
	ii)	**The OIG generally agrees with the CIO on the number of agency owned systems.**		**0**
		a	Yes	0
		b	No	-10
	iii)	**The OIG generally agrees with the CIO on the number of information systems used or operated by a contractor of the agency or other organization on behalf of the agency.**		**0**
		a	Yes	0
		b	No	-10