Section 6: Cybersecurity

Functional Area	Attributes	Traits	Level 1 Basic Capabilities Characteristics	Level 2 Evolving Maturity Characteristics	Level 3 Demonstrated Maturity Characteristics
Cybersecurity	*Functional Area Description: The objective of FITARA is to improve the management of IT within an agency and hence, improve the ability for that agency to deliver its mission and conduct its business. To effectively enable the agency's mission IT must meet the current functional needs as well as evolve to meet the future needs as laid out in the agency's strategic plan. Given the importance of protecting agency data and systems, cybersecurity has become a critical function in the Management of IT, hence its elevation to a function on par with Governance, Budgeting, etc. In fact, cybersecurity must be properly included in all of the other five functions. Every Governance decision needs to consider cybersecurity as a key requirement, budgets must be determined with cybersecurity in mind, all Acquisitions and related Programs must include cybersecurity requirements, and lastly, the need for cybersecurity expertise in an IT organization is now deemed a critical success factor for agencies.* *Through appropriate maturity, an agency can advance its mission through the collaborative development and adoption of enterprise-wide cybersecurity policies matched by prioritized risk management-based implementation of cybersecurity defenses that enable business and mission operations while balancing risk, resource constraints and the need for innovation, and that are subject to clear and measurable performance goals for securing information resources and systems Department-wide.* *Note: Agency means a department or establishment of the Government (compare to bureau). e.g., Treasury is an agency where Enterprise governance would reside. The bureaus under Treasury would include mission specific portfolios and sub-portfolios aligned to the functions of the bureau.*				
	Education and Awareness: Is there adequate understanding across the organization regarding cybersecurity as a priority, and awareness of the threat landscape faced by the Agency?	Cybersecurity is understood to be a shared priority among all stakeholders. Leadership is aware of the evolving threat landscape, broadly as well as in the context of threats that are specific to the agency and/or mission areas	Agency carries out annual cybersecurity awareness training among all staff (federal employees, contractors, and others as applicable). Focus on cybersecurity typically driven across organizations by the Office of the CIO rather than driven from above by Agency and component leadership	Agency broadly carries out role-based training, to include all non-IT professionals who have security-related roles under agency Assessment and Authorization policies, the NIST CSF, etc. Agency leadership briefed on threats on a reactive basis as threats emerge. The topic of cybersecurity is at times part of communications initiated outside of the Office of the CIO	Training and awareness initiatives extend beyond individuals with security-related roles. Leadership is proactively briefed on a periodic basis, to include classified briefings as appropriate. Communications highlighting the importance of cybersecurity are at times initiated at the top of the Agency or components
	Horizontal Integration: Is there proper level of involvement from all appropriate agency stakeholders, including the mission/business leaders, Privacy Officer, General Counsel, and the CIO, CAO, CFO, CHCO (the	Key stakeholder representation of Mission, Business, IT and related support areas like Finance, Acquisition, Legal etc. in decision-making	Ad Hoc participation of executives from the agency in cybersecurity risk determination and prioritization activities. Not well integrated into the agency's governance processes	Appropriate representation and participation from mission, business and IT to meet agency needs. There is active, but not full, participation from other stakeholders in cybersecurity activities.	All proper stakeholders involved with active participation to drive mission aligned, cost effective cybersecurity decisions, with the use of a robust governance process. Cybersecurity addressed as part of planning for major

Functional Area	Attributes	Traits	Level 1 Basic Capabilities Characteristics	Level 2 Evolving Maturity Characteristics	Level 3 Demonstrated Maturity Characteristics
	CXOs) etc.? Is there proper understanding of the cybersecurity threats and vulnerabilities to the agency? Are mission and business owners involved in setting priorities based on the use of the NIST Cybersecurity Framework (NIST CSF)?			Cybersecurity addressed as part of planning for major acquisitions and/or major investments	acquisitions and/or major investments, as well as at the agency and mission level as part of the Agency annual budget formulation process
		Executive-level participation in enterprise risk management use of the NIST Cybersecurity Framework	Senior agency leadership participation is limited and participation is irregular. Cybersecurity not effectively incorporated into Agency enterprise risk management program. The Agency has not embraced the use of the NIST CSF across all functions	Senior agency leadership participation includes regular participation in the use of the NIST CSF	Highest level executives within the agency are actively engaged in enterprise level decision-making using the NIST CSF
	Vertical Integration: Is there completeness and linkage from Enterprise Cybersecurity (overarching strategy of an agency) to Portfolio Cybersecurity (the appropriate grouping of mission/business activities of an agency to Cybersecurity at a Program Level (oversight for program planning and execution activities)? Is the use of the NIST CSF decision making process recognized and adhered to throughout?	Governance structure for Cybersecurity is linked across enterprise, portfolio, and program levels	Partially accounts for enterprise, portfolio, and program level cybersecurity governance; governance set up at all levels but the decision making alignment across the levels is nascent	Enterprise, portfolio, and program level governance for cybersecurity in place; but the decision making alignment across the levels is still under development	Enterprise, portfolio, and program cybersecurity governance are operational with enterprise, portfolio, and program levels, fully adhering the to the use of the NIST CSF
		Strategic alignment and objective success measures are linked through the use of the NIST CSF	Initial stages of developing a cybersecurity risk management and action plan for the agency, with objectives and success measures to drive decision making	Established cybersecurity risk management and action plan for the agency performance measurement and monitoring are in the early stages of initiation at the enterprise, portfolio, and program levels	Established cybersecurity risk management and action plan for the agency performance measurement and monitoring are mature at the enterprise, portfolio, and program levels

Section 6: Cybersecurity

Functional Area	Attributes	Traits	Level 1 Basic Capabilities Characteristics	Level 2 Evolving Maturity Characteristics	Level 3 Demonstrated Maturity Characteristics
	(Caveat: for small agencies, it may be possible to combine enterprise and portfolio governance)	Agency has a robust risk management program in place	Agency has a comprehensive risk management process but it is not used consistently at all levels of governance	Agency has a comprehensive risk management process but that is used at all levels of governance but does not cover all programs	Agency has a comprehensive and well documented risk management process in place supporting all levels of governance and all programs
	Use of the NIST Cybersecurity Risk Management Framework: Does the agency have a comprehensive risk management approach using the NIST CSF as guidance, to include risk identification and impact assessment, risk prioritization analysis, risk mitigation, and risk reporting? Are risks considered in all levels of governance? Does the agency also have a comprehensive approach to cover the lifecycle functions of the NIST CMF, to include Identify, Protect, Detect, Respond, and Recover? Are customers' specialized needs and ways of doing business properly addressed as part of the risk management approach?	Risks are integrated into agency decision-making properly balancing the need for security with tailoring, wherever possible, customers' specialized needs and ways of doing business. The value proposition for cybersecurity measures must be clear to stakeholders. Furthermore, continuous process improvements from both sides, cybersecurity defenders and customers, is required for long-term success	Risks are clearly understood by senior agency leadership. Decision-making focuses on risks proactively. Prioritization is based on a balanced set of factors, including probability, degree of impact, past history and interdependencies	Risks are clearly understood at enterprise and portfolio levels of governance. Decision-making focuses on proactive management of risks. Prioritization is based on a balanced set of factors, including probability, degree of impact, past history and interdependencies Cybersecurity measures are in alignment with and tailored for meeting customer/business needs. Specifically, iterative processes are utilized to solicit customer input/feedback and to determine and understand customer requirements and challenges	Risks are clearly understood at all levels of governance. Decision-making focuses on proactive management of risks. Prioritization is based a balanced set of factors, including probability, degree of impact, past history and interdependencies Cybersecurity measures are in alignment with and tailored for meeting customer and business needs. Specifically, iterative processes are utilized to solicit customer input/feedback and to determine and understanding customer requirements and challenges. Continuous process improvement activities for both cybersecurity defenders and customers ensures long-term success of these program efforts
		Agency fully covers the five lifecycle functions of the NIST CMF, to include Identify, Protect, Detect, Respond, and Recover.	Agency has ad hoc processes in place to address some or all of the five lifecycle functions of the NIST CMF	Agency has processes in place to address all of the five lifecycle functions of the NIST CMF, but is not fully implemented across all horizontal and vertical	Agency has processes in place to address all of the five lifecycle of the NIST CMF, and is fully integrated horizontally and

Section 6: Cybersecurity

Functional Area	Attributes	Traits	Level 1 Basic Capabilities Characteristics	Level 2 Evolving Maturity Characteristics	Level 3 Demonstrated Maturity Characteristics
				elements of the enterprise	vertically across the enterprise
		Agency fully implements the NIST CMF 7 step process, resulting in a comprehensive Action Plan for the enterprise that is regularly updated.	Agency has ad hoc processes in place in developing plans to address cybersecurity risks and vulnerabilities	Agency has implemented the 7-step process, but is not fully implemented across all horizontal and vertical elements of the enterprise	Agency has implemented the 7-step process, and is fully integrated horizontally and vertically across the enterprise
		Agency demonstrates responsible stewardship regarding cybersecurity resources, by correlating resource allocations to measurable metrics and process improvements based on observable results.	Agency has a process for correlating resource allocations for cyber capabilities to measurable metrics	Agency has a process for correlating resource allocations for cyber capabilities to measurable metrics and also documents process improvements based on observable results	Agency has a process for correlating resource allocations for cyber capabilities to measurable metrics and also documents process improvements based on observable results. Agency ensures process improvements are implemented in accordance with the NIST CMF 7 step process
		The agency has mechanisms in place to monitor and response to cyber threats, providing CIO and leadership have visibility into Agency .cybersecurity posture	Cybersecurity (policy compliance, assessment and authorization status, and operational security status) assessed by the Office of the CIO, or assessed locally and reported to Office of the CIO. Agency has begun implementing automated Security Assessment Tools for continuous monitoring and a security operations center (SOC) provides continuous monitoring and diagnostics of IS posture	The agency has implemented automated Security Assessment Tools for continuous monitoring, reports via CyberScope, and works closely with US-CERT. Briefings to Agency leadership take place periodically	The agency has implemented a fully automated Security Assessment Tools for continuous monitoring, reports via CyberScope, and works closely with US-CERT. Continuous monitoring data are vertically integrated to provide holistic picture of enterprise-wide security posture of Agency, fused with internal/external threat information, with frequent reporting to Agency and component leadership

Section 6: Cybersecurity

Functional Area	Attributes	Traits	Level 1 Basic Capabilities Characteristics	Level 2 Evolving Maturity Characteristics	Level 3 Demonstrated Maturity Characteristics
	Information Security (IS): Does the agency properly recognize and incorporate information security requirements? Does the agency have proactive means in place to keep information security policies and approaches current? Does the agency measure effectiveness of information security outcomes by actively collecting metrics? Does the agency use metrics to improve programs and acquisition processes?	The agency leverages leading IS practices to improvement their IT security posture.	There is a process to review and leverage leading IS practices to be used to make improvements to the agency's IS posture	Some IS process metrics are tracked and there is a process to review and leverage leading IT security practices to be used to make improvements to the agency's IT security posture	IS process metrics are tracked and there is a process to review and leverage leading IS practices to be used to make improvements to the agency's IT security posture
		The agency has aligned IS policies with organizational levels, performs assessments, provides training, uses metrics actively to measure effectiveness of IS outcomes and improve programs.	The agency has stand-alone IS policies and procedures, addresses assessments and training to meet minimal requirements. The agency collects metrics only as required for FISMA and Cross Agency Priority (CAP) Goal reporting	The agency has established a linkage between IS policies at each level in the agency, actively assesses risks, and collects metrics for FISMA and CAP Goal reporting. Assessments and risk management are key IT responsibilities	The IS program fully supported throughout the agency, has integrated IS into agency's mission and performance measures, has a robust IS training, collects metrics for FISMA and CAP Goal reporting and uses them used for continuous IS process improvement
		There are modernization efforts to replace antiquated and insecure networks and infrastructure, and to improve resilience of legacy applications	The agency is working to secure funding to implement incremental modernization efforts to replace insecure networks, infrastructure, and legacy applications. Prioritization of resources for modernization may be driven more by potential cost savings than prioritized based on IS risks/exposure	The agency is working to secure funding and schedules incremental modernization efforts to replace insecure networks, infrastructure, and legacy applications. IS risks factor into prioritization decisions relating to allocation of funds for modernization	The agency has secured funding and is incrementally implementing modern infrastructure to replace insecure networks, infrastructure, and legacy applications
		The agency has integrated IS into IT programs	The agency has included IS upfront in some programs, leveraging CIO EA and standards	The agency has included IS upfront in most programs, leveraging CIO EA and standards	The agency has fully integrated IS in all programs, leveraging CIO EA and standards
		IS requirements are integrated into the system development lifecycle.	Security defects are found and addressed during final testing of program. Program implementations delayed due to minimal	Most security defects are found during development. Post-production defects are reduced. Program implementations	Security is incorporated throughout the system development lifecycle to eliminate the

Section 6: Cybersecurity

Functional Area	Attributes	Traits	Level 1 Basic Capabilities Characteristics	Level 2 Evolving Maturity Characteristics	Level 3 Demonstrated Maturity Characteristics
			security requirements defined early, delaying ability to obtain Authority to Operate.	completes security requirements to obtain Authority to Operate.	majority of post-production defects.
		The agency includes IS and supply chain risk management requirements in IT procurements	The agency includes IS requirements in IT procurements	The agency includes IS and supply chain risk management requirements in IT procurements	The agency includes IS and supply chain risk management requirements and evaluation factors in IT procurements and there is a continual process to assess and improve IS requirements for IT procurements
		The agency has an approach to ensure that IT security policies and approaches for programs and acquisitions are kept current	There is some IT security process metric tracking and there is a review process to leverage leading IT security practices	There is IT security process metric tracking and there is a review process to leverage leading IT security practices	IT security process metrics are tracked and there is a process to review and leverage leading IT security practices to be used to make improvements to the Agency's IT security policies, approaches and IT programs and acquisitions
		Metrics are used to measure effectiveness of IT security outcomes and improve acquisition processes	IT security measures are defined but collection and use of measures varies by program and acquisitions	The agency has initiated integration of IS measures and analysis into program strategies and acquisitions for development, implementation, operations and procurements	The agency has fully integrated IS measures and analysis into program strategies and acquisitions for development, implementation, operations and procurements