FireEye Comments on NIST 800-171B

3.11.5e Assess, test, and validate the effectiveness of security controls and specific solutions on a continuous basis through the combination of automated security instrumentation capabilities and human-led testing to identify and address anticipated risk to the system and the organization based on current and accumulated threat information and threat intelligence.

DISCUSSION

Sophisticated threat actors are constantly changing their TTPs (Tools, Techniques, and Procedures); the threat awareness and risk assessment of the organization must therefore also be dynamic, continuous, and automated to keep up with the adversary. Threat intelligence (i.e., threat information that has been aggregated, transformed, analyzed, interpreted, or enriched to provide the necessary context for decision-making processes) is leveraged to enable the automated testing to be appropriate for each specific environment. This process possesses the ability to utilize standardized frameworks as well as current and relevant, threat actor tools, techniques and procedures (TTPs) to measure how current security controls behave against current threats, thus adapting to changes in both in threat actor behavior and changes to the current cyber defenses. The automated security controls instrumentation capability as well as periodic human-led testing provide specific, measured evidence that enables the organization to identify and detect risks as well as create evidence-based recommendations to close gaps in the cyber defenses. Additionally, this capability enables the enterprise to benefit from (1) a *penetration resistant architecture*; (2) *damage limiting operations*; and (3) maximum *cyber resiliency* and *survivability*.

FireEye Comments on NIST 800-171B

SUGGESTED, RELATED, CHANGES TO APPENDIX D-11

APPENDIX D-11 AS PUBLISHED

SECURITY REQUIREMENTS	NIST SP 800 53 *Relevant Security Controls*	
3.11.5e Assess the effectiveness of security solutions at least annually to address anticipated risk to the system and the organization based on current and accumulated threat intelligence.	RA-3	Risk Assessment
	RA-3(3)	Risk Assessment *Dynamic Threat Awareness*

APPENDIX D-11 W/SUGGESTED CHANGES

SECURITY REQUIREMENTS	NIST SP 800 53 *Relevant Security Controls*	
3.11.5e Assess, test and validate the effectiveness of security controls and specific solutions on a continuous and regular basis through the combination of an automated security controls instrumentation capability and annual testing to identify, detect and anticipate risk to the system and the organization based on current and accumulated threat information and threat intelligence.	RA-3(3)	Risk Assessment | Dynamic Threat Awareness
	CA-2(1)	Security Assessments | Independent Assessors
	CA-7(1)	Continuous Monitoring | Independent Assessment
	CA-7(2)	Continuous Monitoring | Trend Analysis
	CA-8(1)	Penetration Testing | Independent Penetration Agent or Team
	CA-9(1)	Internal System Connections | Security Compliance Checks
	CM-4(2)	Security Impact Analysis | Verification of Security Functions
	SR-6(1)	Supplier Reviews | Penetration Testing and Analysis
	SA-12(8)	Supply Chain Protection | Use of All-Source Intelligence
	SA-12(11)	Supply Chain Protection | Penetration Testing / Analysis of Elements, Processes, And Actors
	SA-12(15)	Supply Chain Protection | Processes to Address Weaknesses or Deficiencies

3.12.2e Implement an automated security instrumentation capability enabling the measured and continuous validation of the effectiveness of production security controls, policies and overall system management. This capability leverages threat information, threat intelligence and standard frameworks to maximize effectiveness and facilitate interoperability, flexibility, and automation.

DISCUSSION

The combination of the growing complexity of security ecosystems, the constantly changing and increased sophistication of adversaries and the expanding risk of system configurations digressing from a known good state make it critical that organizations have a method to continuously test and validate security controls to provide measured metrics of effectiveness. The continuous testing of active defenses is enabled by the use of an automated security instrumentation capability. This capability automates the use of actual adversary Tools, Techniques, and Procedures (TTPs), via standard frameworks, against live defenses, enables the enterprise to accurately assess, and measure, the efficacy of today's attacks against today's defenses. In addition to the automated and continuous testing, annual penetration testing will remain valuable for many reasons, including the need to assess organizational defenses against attack types such as physical penetration and social engineering.

An automated security instrumentation capability provides continuous validation of the network, email, end point and cloud security controls. This creates continuous, measured, awareness of actual defensive function. This is delivered, in aggregate, by the instrumentation capability being able to:

- Safely utilize current threat actor TTPs against the production security infrastructure.
- Test and validate that new security controls, or changes to existing controls, are working as intended.
- Identify new security gaps resulting from "drift" in the configuration of defenses.
- Identify new security gaps resulting from new threat actor TTPs.
- Recommend fixes, or modifications, that will close identified gaps.

- Provide measured evidence of defensive function that document the state of security controls across Network, End Point, Email, and Cloud.

SUGGESTED CHANGES TO APPENDIX D-12

APPENDIX D-12 AS PUBLISHED

TABLE D-12: MAPPING SECURITY ASSESSMENT REQUIREMENTS TO CONTROLS

SECURITY REQUIREMENTS	NIST SP 800-53 *Relevant Security Controls*	
3.12.1e Conduct penetration testing at least annually, leveraging automated scanning tools and ad hoc tests using human experts.	CA-8	Penetration Testing
	SR-6(1)	Supplier Reviews *Penetration Testing and Analysis*

APPENDIX D-12 W/SUGGESTED CHANGES

SECURITY REQUIREMENTS	NIST SP 800 53 *Relevant Security Controls*	
3.12.1e Conduct penetration testing at least annually, leveraging automated scanning tools and ad hoc tests using human experts.	CA-8	Penetration Testing
	SR-6(1)	Supplier Reviews *Penetration Testing and Analysis*
3.12.2e Implement an automated security controls instrumentation capability enabling the measured, continuous, daily validation of the effectiveness of security controls, policies and overall system management, leveraging threat information, threat intelligence and standard frameworks.	CA-2(1)	Security Assessments | Independent Assessors
	CA-7(1)	Continuous Monitoring | Independent Assessment
	CA-7(2)	Continuous Monitoring | Trend Analysis
	CA-8(1)	Penetration Testing | Independent Penetration Agent or Team
	CA-9(1)	Internal System Connections | Security Compliance Checks
	CM-4(2)	Security Impact Analysis | Verification of Security Functions
	SR-6(1)	Supplier Reviews | Penetration Testing and Analysis
	SA-12(8)	Supply Chain Protection | Use of All-Source Intelligence
	SA-12(11)	Supply Chain Protection | Penetration Testing / Analysis of Elements, Processes, And Actors
	SA-12(15)	Supply Chain Protection | Processes to Address Weaknesses or Deficiencies