CSE 270 W12 Prove
Nicole Lawrence

Risk Metric:

HIGH RISK
MEDIUM RISK
LOW RISK

ISSUE CATEGORY: MILITARY

1. *DARPA releases a public solicitation of proposals for automating software assurance evaluation to determine risk.*
   https://www.militaryaerospace.com/computers/article/16722132/researchers-ask-industry-for-new-test-and-measurement-to-determine-system-risk-in-software-assurance
   Risk: Replacing human evaluators with automated software assurance could miss critical risks that require human imagination and experience to anticipate.
   Variables: human imagination, human experience, limits of automated systems to detect threats.
   Occurrence: Possible
   Severity: Substantial

Chart:

Occurrence						
	Near Certainty					
	Highly Likely					
	Possible				*	
	Unlikely					
	Remote					
		Negligible	Minor	Moderate	Substantial	Severe
		Severity				

Mitigation:

Prevention: Automation results double-checked by human evaluators could be the best-case scenario for removing as much risk as possible in the process.

Acceptance: The most likely course of action, the DoD can determine that the projected benefits of automation outweigh any possible risks.

Avoidance: Continue using human evaluators.

Mitigation Tests:

Prevention:

Action: Enable automation but set up a portion of the risk management team as human evaluators doublechecking the automation results. Compare to pure automation results without human oversight.

Result: More expensive, as human evaluators are still on the payroll.

Effect on Risk: Prove whether automation without human oversight is as effective as utilizing human evaluators.

Acceptance:

Action: None

Result: As much as possible, the software assurance evaluation process is automated.

Effect on Risk: None

Avoidance:

Action: Cancel the call for automation bids

Result: Continue using human evaluators

Effect on Risk: While this specific risk has been neutralized, the DoD is now back at square one with the previous risk associated with human evaluators.

2. *DoD current use of Agile too slow, ineffective, and impacts national security*
https://www.forbes.com/sites/stevedenning/2019/09/22/how-fake-agile-at-dod-risks-national-security/?sh=28f8134b8fa8
https://breakingdefense.com/2020/06/dod-agile-software-development-still-too-slow-gao/

Risk: Inaccurate application of the Agile methodology in software development projects reduces efficiency, integrity, and waste of government funds.

Variables: software development management, quality assurance management, human evaluators

Occurrence: Highly Likely

Severity: Moderate

Chart:

Occurrence		Negligible	Minor	Moderate	Substantial	Severe
	Near Certainty					
	Highly Likely			*		
	Possible					
	Unlikely					
	Remote					
Severity						

Mitigation:

Avoidance: Change DoD policy regarding application of and training in Agile to ensure best practices are followed. Alternatively, use another methodology with extensive training from the beginning.

Mitigation Tests:

Avoidance:

Action: Implement intensive training for all software development teams and management. Hire necessary instructors/experts to do so.

Result: DoD software developers fully trained in Agile and able to use the methodology to streamline work and increase productivity.

Effect on Risk: Should pull the risk down to negligible levels

CSE 270 W12 Prove
Nicole Lawrence

3. *DoD Information and Communications Technology (ICT) relies on global supply chain infrastructure which can affect the integrity of software and hardware products*
https://idstch.com/threats/dod-gives-thrust-to-supply-chain-risk-management-scrm-to-mitigate-threats-to-ict-supply-chains/

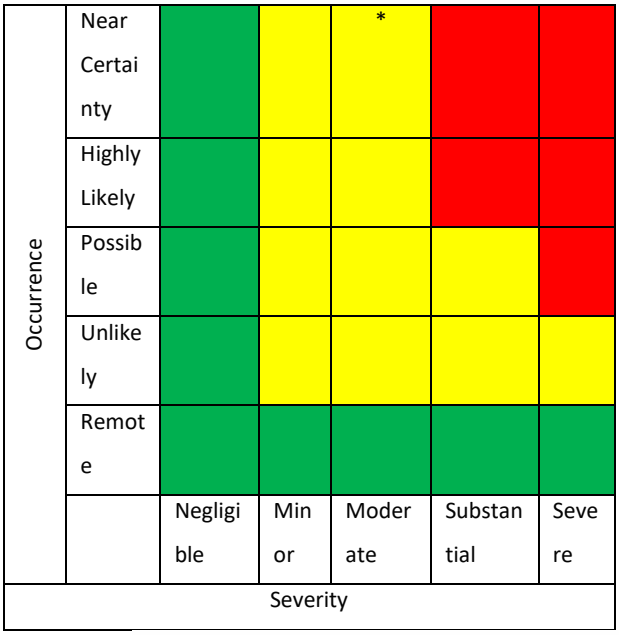
Risk: Inability to control security and product integrity through an increasingly globalized supply chain introduces software, hardware, and human-based vulnerabilities.

Variables: abstraction of information between the tiers of the DoD supply chain, software vulnerabilities, hardware vulnerabilities

Occurrence: Near Certainty

Severity: Moderate

Chart:



Mitigation:

Prevention: Strict compliance requirements through all private sector supply pipelines. Increased communication and information-sharing will reduce time spent in development and production. An effective management system that tracks, supports, and guides all suppliers to provide the best product.

Acceptance: Accepting the possible risk since most attacks (regardless of occurrence) will range from negligible to moderate in severity, not affecting the supply chain beyond projected acceptable losses.

Mitigation Tests:

Prevention:

Action: More government oversight on private sector supply pipelines, increased coordination between tiers of the supply chain, creating a management system to implement both.

Result: More cost with hiring managers, processing security clearances, evaluating need-to-know levels of access to classified information, possible loss of suppliers who do not wish to comply with increased requirements.

Effect on Risk: Could pull the risk occurrence down to 'Possible' and severity down to moderate.

Acceptance:

Action: None

Result: Current vulnerabilities remain and more are possibly created and exploited.

Effect on Risk: Risk level remains the same or increases in severity.

CSE 270 W12 Prove
Nicole Lawrence

4. *DoD canceling cloud computing Joint Enterprise Defense Infrastructure (JEDI) in favor of new solicitation for proposals: Joint Warfighter Cloud Capability (JWCC)*
https://breakingdefense.com/2021/07/dod-cancels-jedi-pivots-to-jumpstart-enterprise-cloud/

Risk: Despite any deficiencies in the JEDI system, the commercial enterprise cloud computing systems the DoD is inviting to bid on JWCC have been repeatedly hacked by domestic and foreign agents.

(Side issue: Getting rid of a system with the awesome acronym of JEDI sends the wrong message about our country)

Variables: security of potential enterprise cloud computing systems, legal holdups like those that occurred when Microsoft was awarded the contract for JEDI

Occurrence: Possible

Severity: Moderate

Chart:

Occurrence		Negligible	Minor	Moderate	Substantial	Severe
	Near Certainty					
	Highly Likely					
	Possible			*		
	Unlikely					
	Remote					
	Severity					

Mitigation:

Prevention: Have security requirements and guidelines laid out before awarding the JWCC contract.

Acceptance: Acknowledge the potential risks as unavoidable no matter which company DoD contracts with for enterprise cloud computing

Avoidance: Stick with JEDI (and that awesome acronym) and adjust it according to lessons learned instead of switching tracks before JEDI's full potential can be explored.

Mitigation Tests:

Prevention:

Action: Effective requirements and guidelines researched, written, and reviewed.

Result: Extra expenses and time before any contract can be awarded. Potential slowdown of service.

Effect on Risk: Reduce risk significantly but not out of the medium level.

Acceptance:

Action: None

Result: Risk remains the same.

Effect on Risk: None

Avoidance:

Action: institute a system-wide evaluation of the JEDI system to identify where it can be refined and made faster and more secure.

Result: Possible slowdown of service. Extra expenses and time to review and institute changes.

Effect on Risk: Unknown if retaining and revising JEDI will yield lower risk than JWCC

5. *China likely culprit for latest high-profile cyber-attack, further straining already-tenuous US/China relations*
   https://breakingdefense.com/2021/07/government-to-attribute-exchange-hacks-soon/
   Risk: China becoming more emboldened in increasingly effective cyber-attacks and continued deterioration of US/China relations negatively impacting national security and foreign policy.
   Variables: Chinese interest in US military and corporate secrets, current security of those secrets
   Occurrence: Near Certainty
   Severity: Severe

Chart:

Occurrence						
	Near Certainty					*
	Highly Likely					
	Possible					
	Unlikely					
	Remote					
		Negligible	Minor	Moderate	Substantial	Severe
		Severity				

Mitigation:

Prevention: Increased cybersecurity for any classified information and clear consequences for China if attacks continue.

Acceptance: Accepting that foreign cyberattacks will occur and hoping nothing too important is stolen or compromised.

Mitigation Tests:

Prevention:

Action: Increase security measures, increase consequences for China from the United States and, possibly, on an international stage (UN or other international coalitions)

Result: Increased tension in China/US relations and, possibly, relations between the US and other countries. The risk of having to enforce consequences and military/economic repercussions.

Effect on Risk:

Acceptance:

Action: None

Result: Possible further risks created as continued cyberattacks discover/create more vulnerabilities and compromised classified data.

Effect on Risk: Risk will stay at max threat level.