REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*
08/11/2020

2. REPORT TYPE
Conference Briefing

3. DATES COVERED *(From - To)*

4. TITLE AND SUBTITLE
Information Brief: Widget Deliveries Cybersecurity Risk Assessment Methodology

5a. CONTRACT NUMBER
W56KGU-19-D-0004

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Christopher M Wiehe (MITRE)
Bill Farnsworth (Northrop Grumman Space Systems)

5d. PROJECT NUMBER
0719B1GMGR

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
The MITRE Corporation
7515 Colshire Drive
McLean, VA 22102

8. PERFORMING ORGANIZATION REPORT NUMBER
PRS-20-2071;
20 MDA 10550 (10 Aug 20)

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
United States Army (ACC-APG)

10. SPONSOR/MONITOR'S ACRONYM(S)
ACC-APG

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.

13. SUPPLEMENTARY NOTES
Preprint to Northrop Grumman Cyber Summit

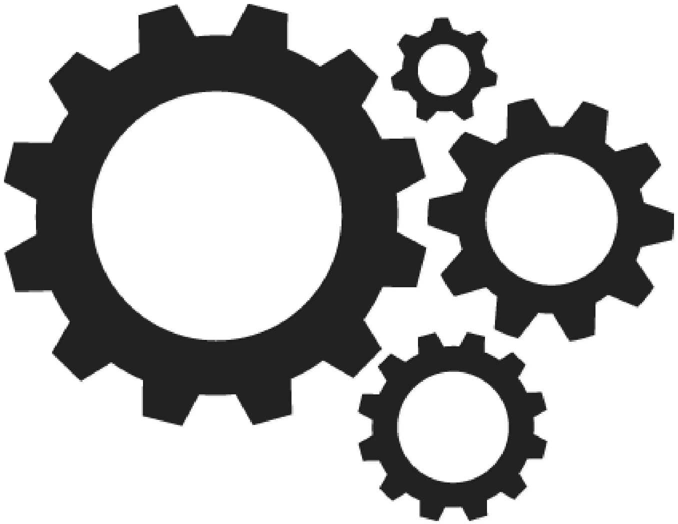
14. ABSTRACT
Provide an Overview of the Widget Deliveries Cybersecurity Risk Assessment Methodology

15. SUBJECT TERMS
Computer Security; Risk Management; risk assessment; cybersecurity; widget deliveries; attack execution; resiliency

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			Susan Carpenito
				24	**19b. TELEPHONE NUMBER** *(Include area code)* 781-271-7646

Information Brief
Widget Deliveries Cybersecurity Risk Assessment Methodology

This technical data deliverable was developed using contract funds under Basic Contract No. W56KGU-19-F-0004.



Cybersecurity Division

Presented By:
Mr. Chris Wiehe, The MITRE Corporation
Mr. Bill Farnsworth, Northrop Grumman Space Systems

31 July 2020

Purpose

Provide an Overview of the Widget Deliveries Cybersecurity Risk Assessment Methodology

Background

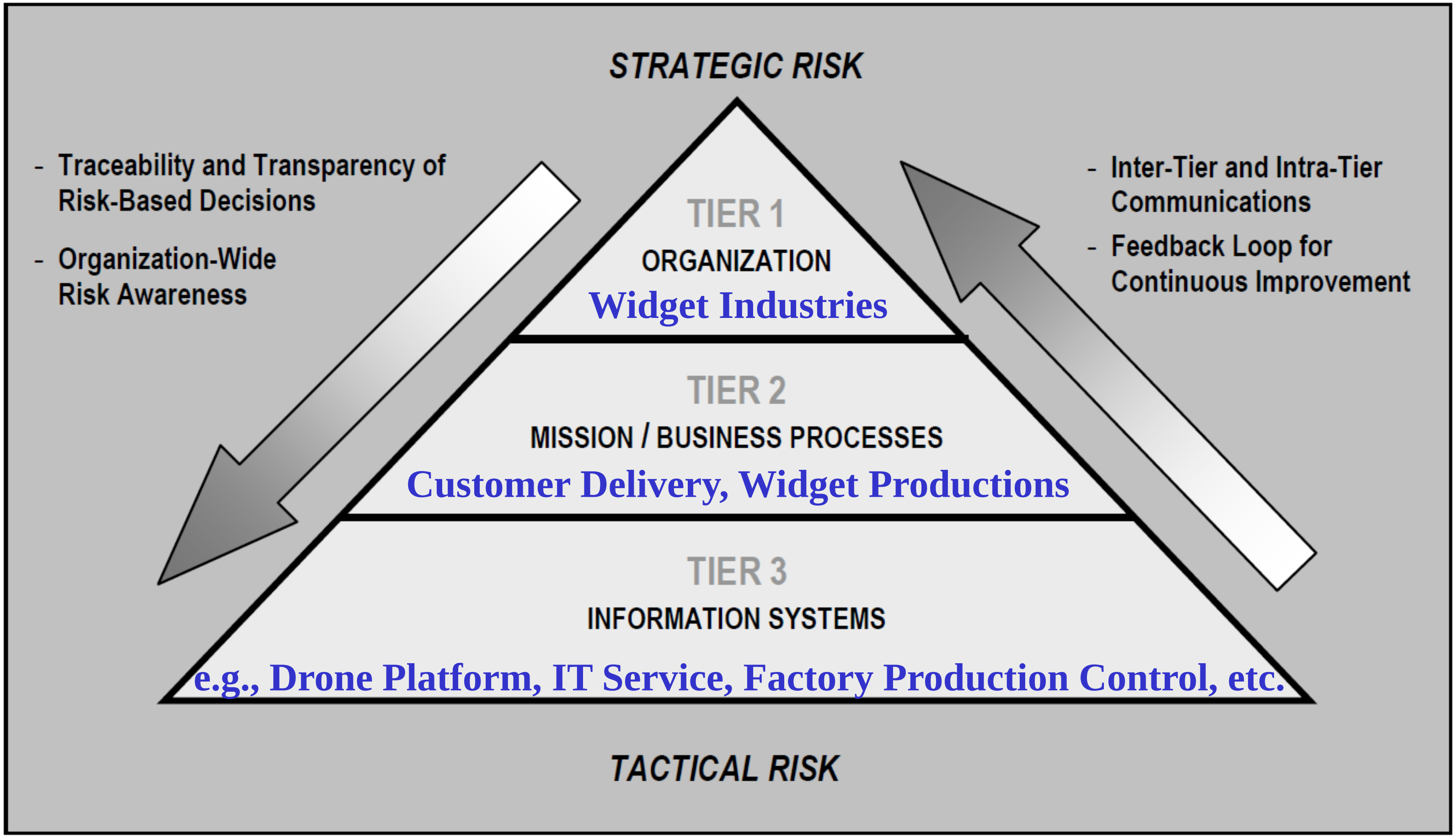
- **Widget Deliveries CEO requested development of Cybersecurity Risk Process to enable project managers (PMs) to make risk based decisions**
- **Cybersecurity Division coordinated with stakeholders for development based upon:**
  - **NIST SP 800-30r1**
  - **Industry Best Practices for Risk Assessments**
- **Risk process has been updated to define criteria and restructure Risk Attributes**
  - **Primary process structure remains consistent**
  - **Addressed early inconsistencies with risk outcomes**
- **Process approved at technical review by Widget Deliveries CEO (31 Dec 18)**

Widget Deliveries Cybersecurity Risk Assessment methodology adheres to all applicable laws

Cybersecurity Risk is Qualitative

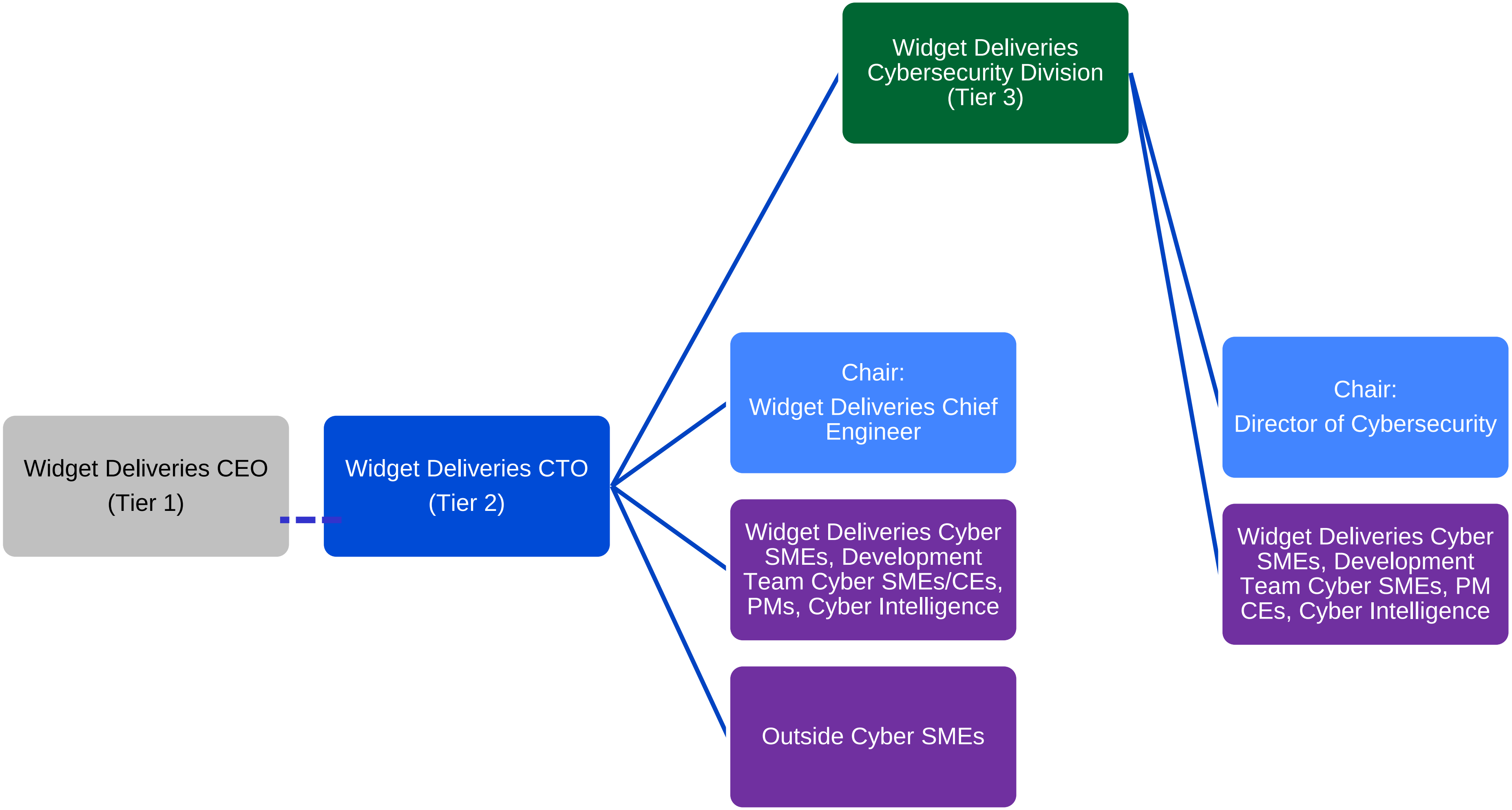
- Many competing approaches exist to score and quantify risk
  - All are subjective
- Quantification supports determining relative risk and prioritization, NOT absolute risk
- Characterizing mission consequence and the likelihood that a given attack succeeds is essential
- Measuring cyber impact/consequences is not a science
  - Attack campaigns can be multi-pronged, over long durations and multifaceted
  - Cyber is not deterministic
- Currently we rely on SME knowledge for likelihood characterization of attack vectors and effectiveness
- Chief engineers expertise needed to help PMs prioritize amongst risks of different types

Widget Deliveries Risk Hierarchy


STRATEGIC RISK
- Traceability and Transparency of Risk-Based Decisions
- Organization-Wide Risk Awareness
- Inter-Tier and Intra-Tier Communications
- Feedback Loop for Continuous Improvement
TIER 1
ORGANIZATION
Widget Industries
TIER 2
MISSION / BUSINESS PROCESSES
Customer Delivery, Widget Productions
TIER 3
INFORMATION SYSTEMS
e.g., Drone Platform, IT Service, Factory Production Control, etc.
TACTICAL RISK

Derived from NIST 800-30R1, Figure 4

Widget Deliveries Cybersecurity Risk Board Organization



Widget Deliveries CEO (Tier 1)

Widget Deliveries CTO (Tier 2)

Widget Deliveries Cybersecurity Division (Tier 3)

Chair: Widget Deliveries Chief Engineer

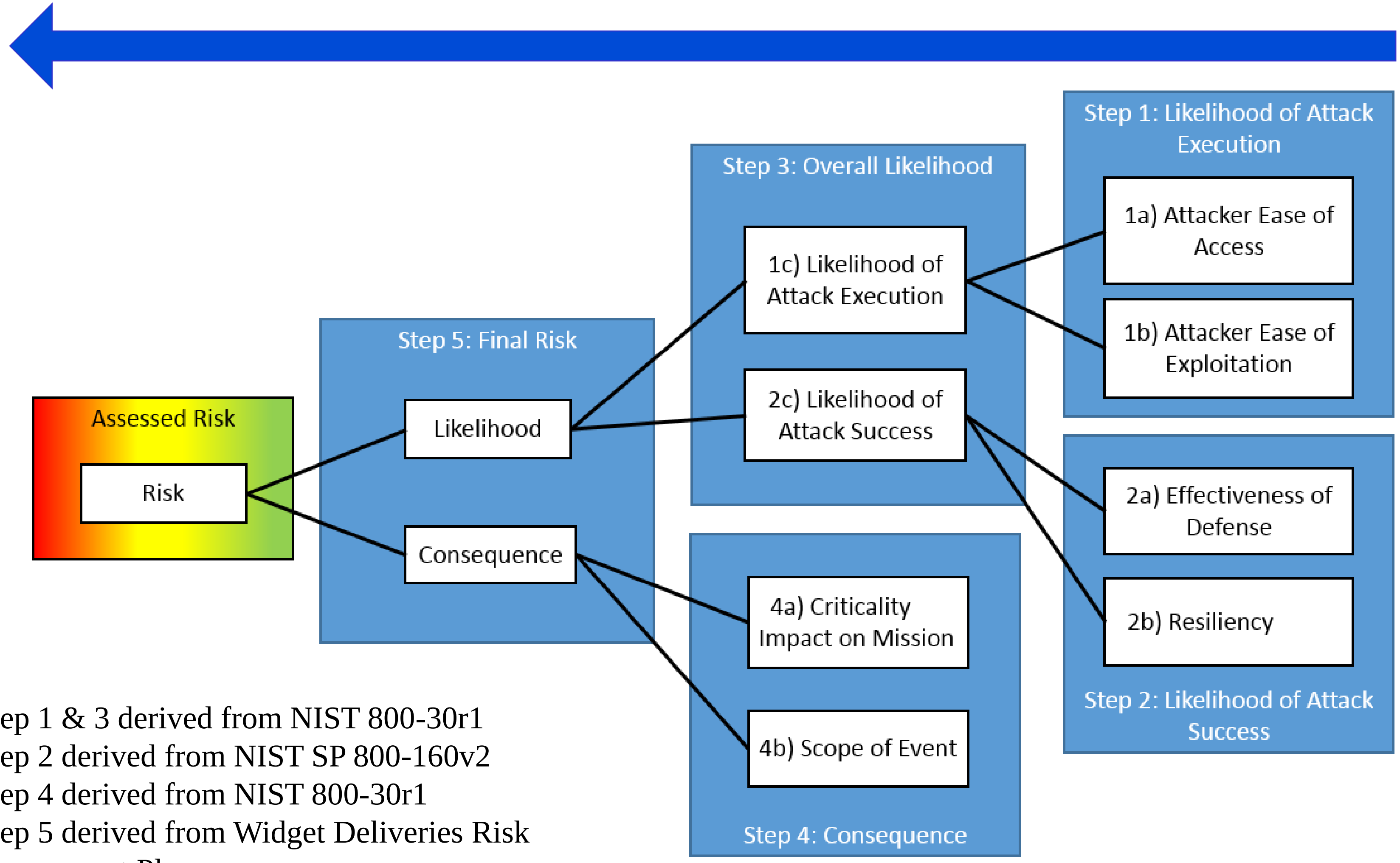
Widget Deliveries Cyber SMEs, Development Team Cyber SMEs/CEs, PMs, Cyber Intelligence

Outside Cyber SMEs

Chair: Director of Cybersecurity

Widget Deliveries Cyber SMEs, Development Team Cyber SMEs, PM CEs, Cyber Intelligence

Cybersecurity Risk Decomposition

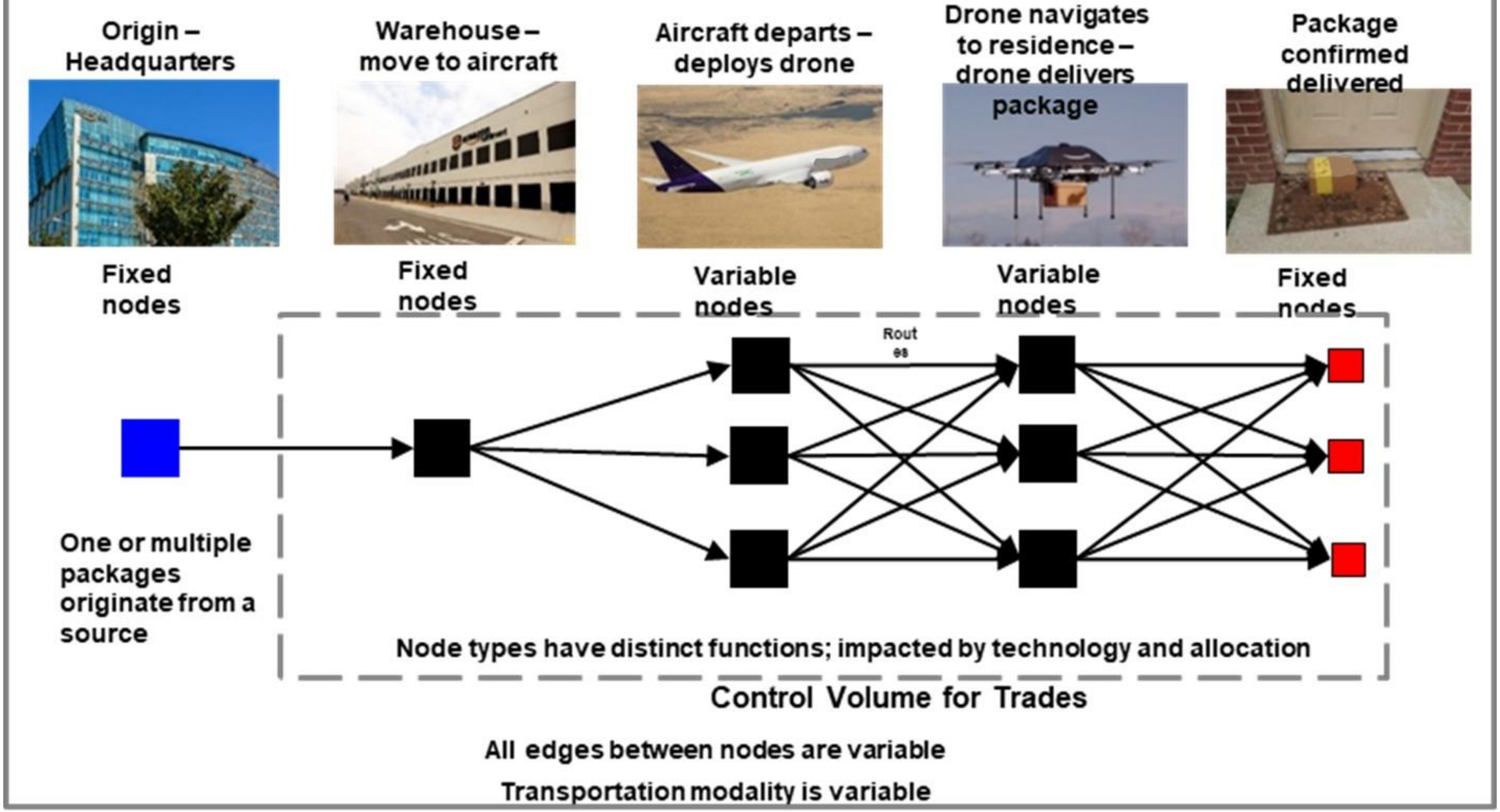


Step 1: Likelihood of Attack Execution
1a) Attacker Ease of Access
1b) Attacker Ease of Exploitation
Step 3: Overall Likelihood
1c) Likelihood of Attack Execution
2c) Likelihood of Attack Success
Step 5: Final Risk
Likelihood
Consequence
Assessed Risk
Risk
2a) Effectiveness of Defense
2b) Resiliency
Step 2: Likelihood of Attack Success
4a) Criticality Impact on Mission
4b) Scope of Event
Step 4: Consequence

-Step 1 & 3 derived from NIST 800-30r1
-Step 2 derived from NIST SP 800-160v2
-Step 4 derived from NIST 800-30r1
-Step 5 derived from Widget Deliveries Risk Management Plan

Widget Deliveries Expedient Delivery Scenario (<1 hour – high value delivery)

2 drones sent for every delivery for reliability



Origin – Headquarters

Warehouse – move to aircraft

Aircraft departs – deploys drone

Drone navigates to residence – drone delivers package

Package confirmed delivered

Fixed nodes

Fixed nodes

Variable nodes

Variable nodes

Fixed nodes

Routes

One or multiple packages originate from a source

Node types have distinct functions; impacted by technology and allocation

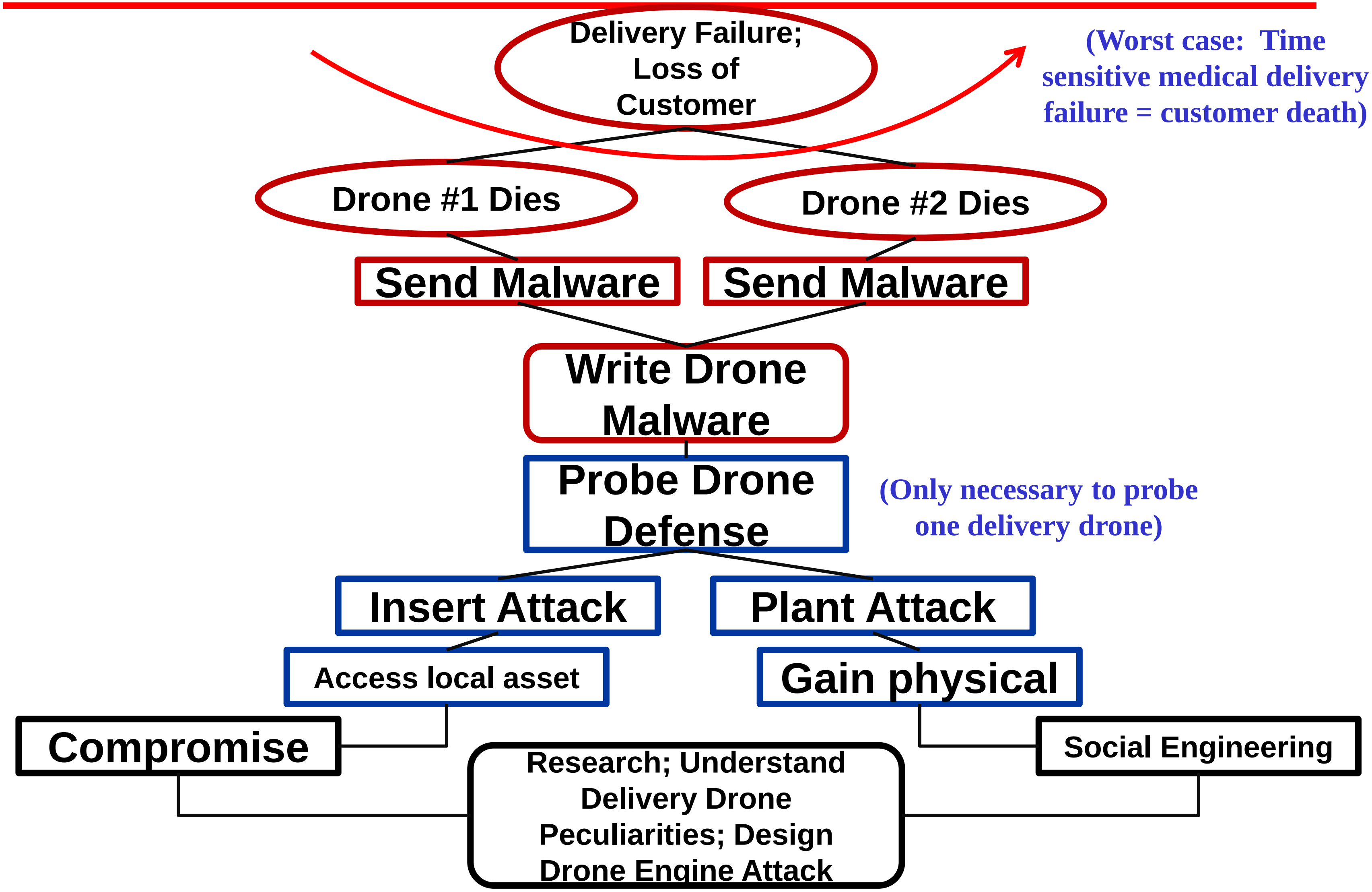
Control Volume for Trades

All edges between nodes are variable

Transportation modality is variable

Modification of original T885/T886 concept

Attack Scenario



Delivery Failure; Loss of Customer

(Worst case: Time sensitive medical delivery failure = customer death)

Drone #1 Dies

Drone #2 Dies

Send Malware

Send Malware

Write Drone Malware

Probe Drone Defense

(Only necessary to probe one delivery drone)

Insert Attack

Plant Attack

Access local asset

Gain physical

Compromise

Social Engineering

Research; Understand Delivery Drone Peculiarities; Design Drone Engine Attack

Preconditions

(Each risk will have their own preconditions listed)

When assessing risk of a cyber threat, preconditions should be taken into consideration to accurately determine the likelihood/consequence rating. Preconditions are circumstances that surround the operational environment that could either increase or decrease exploitation opportunity or effectiveness.

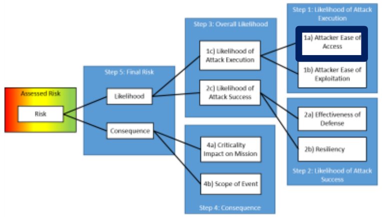
Examples of preconditions that would increase likelihood/consequence may include:

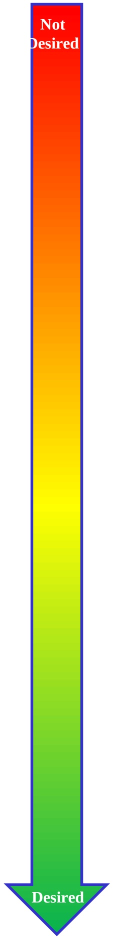
- Vulnerable Graphic User Interface (GUI) /Terminals not in Ops Center
- Multiple GUI users at various locations with potential command line access
- Insiders with single point high access conditions

Examples of preconditions that would decrease likelihood/consequence may include:

- Limited access: Small user pool requiring special access privileges at a single location
- Drones assembled in Super Secure Vault (SSV) open during small timeframes at a single location with multi-person control
- Access limited to field operations group to SSV; 2-person access control
- Small user pool hand-selected for position
- Small user pool with extensive background check required

Step 1a: Attacker Ease of Access Criteria (Likelihood of Attack Execution)


Step 1: Likelihood of Attack Execution
1a) Attacker Ease of Access
1b) Attacker Ease of Exploitation
Step 3: Overall Likelihood
1c) Likelihood of Attack Execution
2c) Likelihood of Attack Success
Step 5: Final Risk
Likelihood
Consequence
Assessed Risk
Risk
Step 2: Likelihood of Attack Success
2a) Effectiveness of Defense
2b) Resiliency
Step 4: Consequence
4a) Criticality Impact on Mission
4b) Scope of Event



ATTACKER EASE OF ACCESS CRITERIA

Very High (Very Easy)

1. Attack does not require network access.
2. Attacker does not require physical access.
3. An adversary can initiate attack at any time; no restrictions based on time window.
4. User privileges not required.

High (Easy)

1. Attacker requires remote or external network access (includes trusted & external interfaces, e.g., Network Operations Center).
2. Adversary requires escorted physical access to target system.
3. Attack time window limited but frequently occurs.
4. User privileges not required.

Moderate

1. Attacker requires access to any internal network connected to a non-targeted system (e.g., any Widget Deliveries network spoke).
2. Adversary requires unescorted physical access to a non-targeted computing asset.
3. Attack time window is limited but adversary can control.
4. User privileges not required.

Low (Difficult)

1. Attacker requires access to the network connected to the targeted system (e.g., Widget Deliveries network hub or local subnet).
2. Adversary requires unescorted physical access to the targeted computing asset.
3. Attack time window is very limited but is still known to the adversary.
4. Attacker requires user or admin privileges.

Very Low (Very Difficult)

1. Attacker requires direct access to target system, cannot exploit targeted asset via a network connection.
2. Adversary requires unescorted physical access to the targeted computing asset.
3. Attack requires very specific time window to engage & window is unknown to the adversary.
4. Attacker requires administrative privileges.

Attacker is an individual or group of individuals acting with intent to disrupt or deny the mission.

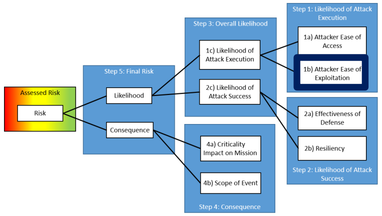
Within the Attacker Ease of Access Criteria, select the attribute level for each of the following:

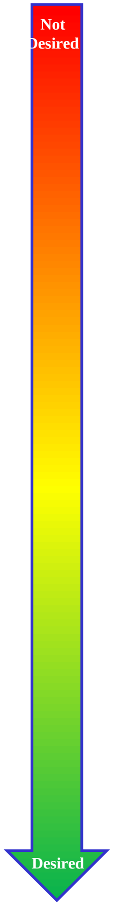
1. Network access
2. Physical access
3. Time window
4. Type of privilege

Results for Attacker Ease of Access is: <u>{Insert Level}</u>

- Justification for determined likelihood needs to be specific to the system being assessed

Step 1b: Attacker Ease of Exploitation Criteria (Likelihood of Attack Execution)


Assessed Risk
Risk
Step 5: Final Risk
Likelihood
Consequence
Step 3: Overall Likelihood
1c) Likelihood of Attack Execution
2c) Likelihood of Attack Success
Step 4: Consequence
4a) Criticality Impact on Mission
4b) Scope of Event
Step 1: Likelihood of Attack Execution
1a) Attacker Ease of Access
1b) Attacker Ease of Exploitation
Step 2: Likelihood of Attack Success
2a) Effectiveness of Defense
2b) Resiliency



Exploitation is the act of trying to turn a vulnerability (weakness) into an actual way to breach a system.

Within the Attacker Ease of Exploitation Criteria, select the attribute level for each of the following:

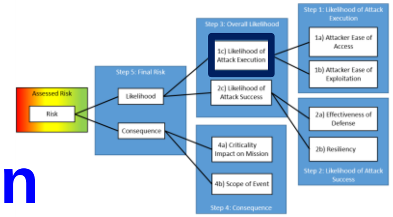
1. General technical cyber-attack knowledge
2. Specific system knowledge/configurations
3. Exploitation tools required

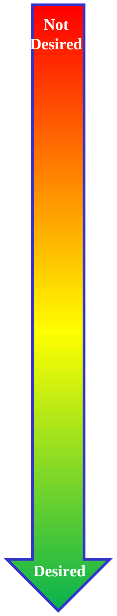
Results for Attacker Ease of Exploitation is: {Insert Level}

- Justification for determined likelihood needs to be specific to the system being assessed

ATTACKER EASE OF EXPLOITATION CRITERIA
Very High (Very Easy) 1. No cyber-attack technology knowledge required. 2. No specific Widget Deliveries system knowledge required. 3. Well-known vulnerabilities or configuration weaknesses are present and exploitation tools are readily available.
High (Easy) 1. Generic/Common cyber-attack technology knowledge required. 2. Some basic Widget Deliveries system component knowledge required. 3. Existing exploitation tools are readily available.
Moderate 1. Low-level cyber-attack technology knowledge required. 2. Some knowledge of targeted systems and its configuration is required. 3. General purpose exploitation tools are difficult to obtain and must be tailored to the system.
Low (Difficult) 1. Mid-level cyber-attack technology knowledge required. 2. Detailed knowledge of target system is required (discoverable through significant proprietary information or privileged access). 3. Multi-faceted exploitation tools and orchestration required.
Very Low (Very Difficult) 1. High-level cyber-attack technology knowledge required. 2. Detailed knowledge of target system and operations is required. 3. Complex Widget Deliveries system specific attack and orchestration required.

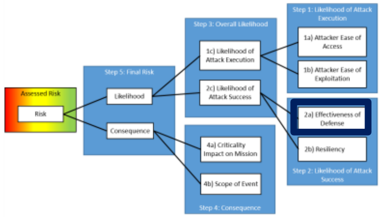
Step 1c: Likelihood of Attack Execution


Assessed Risk
Risk
Step 5: Final Risk
Likelihood
Consequence
Step 3: Overall Likelihood
1c) Likelihood of Attack Execution
2c) Likelihood of Attack Success
Step 4: Consequence
4a) Criticality Impact on Mission
4b) Scope of Event
Step 1: Likelihood of Attack Execution
1a) Attacker Ease of Access
1b) Attacker Ease of Exploitation
Step 2: Likelihood of Attack Success
2a) Effectiveness of Defense
2b) Resiliency

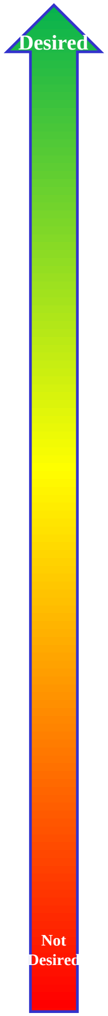


ATTACKER EASE OF ACCESS CRITERIA	ATTACKER EASE OF EXPLOITATION CRITERIA
Very High (Very Easy) Attack does not require network access. Attacker does not require physical access. An adversary can initiate attack at any time; no restrictions based on time window. User privileges not required.	**Very High (Very Easy)** No cyber-attack technology knowledge required. No specific Widget Deliveries system knowledge required. Well-known vulnerabilities or configuration weaknesses are present and exploitation tools are readily available.
High (Easy) Attacker requires remote or external network access (includes trusted & external interfaces). Adversary requires escorted physical access to target system. Attack time window limited but frequently occurs. User privileges not required.	**High (Easy)** Generic/Common cyber-attack technology knowledge required. Some basic Widget Deliveries system component knowledge required. Existing exploitation tools are readily available.
Moderate Attacker requires access to any internal network connected to a non-targeted system. Adversary requires unescorted physical access to a non-targeted computing asset. Attack time window is limited but adversary can control. User privileges not required.	**Moderate** Low-level cyber-attack technology knowledge required. Some knowledge of targeted systems and its configuration is required. General purpose exploitation tools are difficult to obtain and must be tailored to the system.
Low (Difficult) Attacker requires access to the network connected to the targeted system. Adversary requires unescorted physical access to the targeted computing asset. Attack time window is very limited but is still known to the adversary. Attacker requires user or admin privileges.	**Low (Difficult)** Mid-level cyber-attack technology knowledge required. Detailed knowledge of target system is required (discoverable through significant proprietary information or privileged access). Multi-faceted exploitation tools and orchestration required.
Very Low (Very Difficult) Attacker requires direct access to target system, cannot exploit targeted asset via a network connection. Adversary requires unescorted physical access to the targeted computing asset. Attack requires very specific time window to engage & window is unknown to the adversary. Attacker requires administrative privileges.	**Very Low (Very Difficult)** High-level cyber-attack technology knowledge required. Detailed knowledge of target system and operations is required. Complex Widget Deliveries system specific attack and orchestration required.

Matrix (Scale derived from NIST 800-30r1)		**Attacker Ease of Exploitation**				
		Very Low	**Low**	**Moderate**	**High**	**Very High**
Attacker Ease of Access	**Very High**	Low	Moderate	High	Very High	Very High
	High	Low	Moderate	Moderate	High	Very High
	Moderate	Low	Low	Moderate	Moderate	High
	Low	Very Low	Low	Low	Moderate	Moderate
	Very Low	Very Low	Very Low	Low	Low	Low


Step 1: Likelihood of Attack Execution
1a) Attacker Ease of Access
1b) Attacker Ease of Exploitation
Step 2: Likelihood of Attack Success
2a) Effectiveness of Defense
2b) Resiliency
Step 3: Overall Likelihood
1c) Likelihood of Attack Execution
2c) Likelihood of Attack Success
Step 4: Consequence
4a) Criticality Impact on Mission
4b) Scope of Event
Step 5: Final Risk
Likelihood
Consequence
Assessed Risk
Risk

Step 2a: Effectiveness of Defense Criteria



EFFECTIVENESS OF DEFENSE CRITERIA
Very High 1. Protections are fully effective against adversarial attacks. 2. System detects the most sophisticated adversarial attacks. 3. System and operators are able to automatically respond to attacks. 4. Layered defensive (physical and logical) measures are in-place on target system.
High 1. Protections effectively contain and limit attack success**.** 2. System able to detect most types of attacks. 3. System and operators are able to respond to attacks with some delay. 4. Limited layered defensive (physical and logical) measures are in-place target system.
Moderate 1. Protections effectively contain **or** limit attack success. 2. System able to detect some attacks. 3. System **or** operators are able to automatically respond to attacks. 4. Limited layered defensive (physical **or** logical) measures are in-place and verified on target system.
Low 1. Protections may not be fully effective against attacks. 2. Attack evades detection. 3. System **or** operators unable to respond to attacks. 4. Some defensive (physical **or** logical) measures are in-place on target system.
Very Low 1. Protections are ineffective or not implemented against attacks. 2. Attack evades even sophisticated detection. 3. System **or** operators unable to respond to attacks. 4. No defensive (physical **or** logical) measures are in-place on target system.

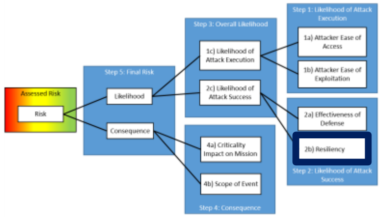
Physical defensive measures can be gates, guards or guns. Logical defensive measures can be access control lists (ACLs) and technical settings applied

Within the Effectiveness of Defense Criteria, select the attribute level for each of the following:

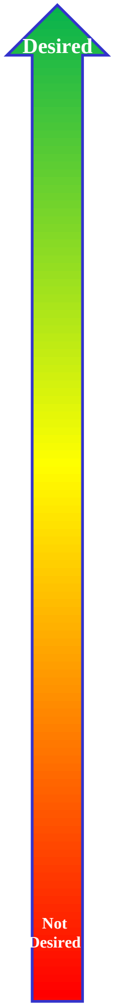
1. Protect
2. Detect
3. Respond
4. Defend

Results for Effectiveness of Defense is: {Insert Level}

- Justification for determined likelihood needs to be specific to the system being assessed


Assessed Risk
Risk
Step 5: Final Risk
Likelihood
Consequence
Step 3: Overall Likelihood
1c) Likelihood of Attack Execution
2c) Likelihood of Attack Success
Step 4: Consequence
4a) Criticality Impact on Mission
4b) Scope of Event
Step 1: Likelihood of Attack Execution
1a) Attacker Ease of Access
1b) Attacker Ease of Exploitation
2a) Effectiveness of Defense
2b) Resiliency
Step 2: Likelihood of Attack Success

Step 2b: Resiliency Criteria



Cyber resiliency is the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources regardless of the source. (NIST SP 800-160v2)

Within the Resiliency Criteria, select the attribute level for each of the following:

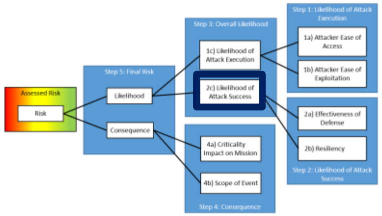
1. Anticipate
2. Withstand
3. Recover
4. Adapt to

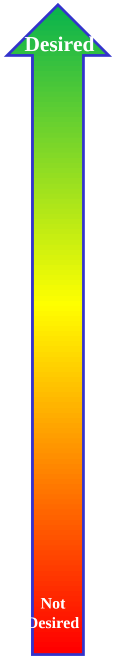
Results for Resiliency is: <u>{Insert Level}</u>

- Justification for determined likelihood needs to be specific to the system being assessed

RESILIENCY CRITERIA
Very High 1. System will anticipate the threat and proactively change the attack surface automatically. 2. Architecture consists of a heterogeneous environment that can withstand sophisticated attacks. 3. System automatically recovers from attack and maintains full operational capability. 4. System adapts to attack automatically (e.g., system will recompile tactical code in real-time or swap to a shadow system).
High 1. System will anticipate the threat and proactively change the attack surface to an alternate capability. 2. Architecture is highly segmented with diversity to withstand attacks. 3. System automatically recovers and maintains partial operational capability. 4. System adapts to attack automatically (e.g., transferring to a pre-planned system configuration).
Moderate 1. System may anticipate some of the threat, however operator changes the attack surface to a degraded alternate capability. 2. Architecture consists of limited diversity to withstand some attacks. 3. System recovers after manual switch-over and maintains full operational capability. 4. System adapts to attack manually (e.g., manual transfer to a pre-planned configuration).
Low 1. System cannot anticipate the threat but operator can change the attack surface to a degraded alternate capability within its enclave. 2. Architecture consists of computing assets that cannot withstand attacks. 3. System partially recovers but does not maintain full operational capability. 4. System adapts to attack manually (e.g., locking-out all users).
Very Low 1. System cannot anticipate the threat and operator unable to change the attack surface. 2. System cannot withstand an attack. 3. System cannot recover from an attack to maintain operational capability. 4. System cannot adapt to an attack.

Step 2c: Likelihood of Attack Success

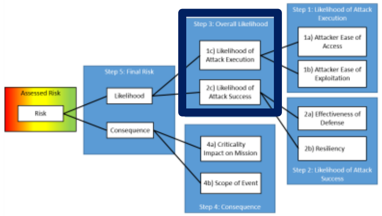

Step 1: Likelihood of Attack Execution
1a) Attacker Ease of Access
1b) Attacker Ease of Exploitation
Step 3: Overall Likelihood
1c) Likelihood of Attack Execution
2c) Likelihood of Attack Success
Assessed Risk
Risk
Step 5: Final Risk
Likelihood
Consequence
2a) Effectiveness of Defense
2b) Resiliency
Step 2: Likelihood of Attack Success
4a) Criticality Impact on Mission
4b) Scope of Event
Step 4: Consequence



EFFECTIVENESS OF DEFENSE CRITERIA	RESILIENCY CRITERIA
Very High Protections are fully effective against adversarial attacks. System detects the most sophisticated adversarial attacks. System and operators are able to automatically respond to attacks. Layered defensive (physical and logical) measures are in-place on target system.	**Very High** System will anticipate the threat and proactively change the attack surface automatically. Architecture consists of a heterogeneous environment that can withstand sophisticated attacks. System automatically recovers from attack and maintains full operational capability. System adapts to attack automatically (e.g., system will recompile tactical code in real-time or swap to a shadow system).
High Protections effectively contain and limit attack success**.** System able to detect most types of attacks. System and operators are able to respond to attacks with some delay. Limited layered defensive (physical and logical) measures are in-place on target system.	**High** System will anticipate the threat and proactively change the attack surface to an alternate capability. Architecture is highly segmented with diversity to withstand attacks. System automatically recovers and maintains partial operational capability. System adapts to attack automatically (e.g., transferring to a pre-planned system configuration).
Moderate Protections effectively contain **or** limit attack success. System able to detect some attacks. System **or** operators are able to automatically respond to attacks. Limited layered defensive (physical **or** logical) measures are in-place and verified on target system.	**Moderate** System may anticipate some of the threat, however operator changes the attack surface to a degraded alternate capability. Architecture consists of limited diversity to withstand some attacks. System recovers after manual switch-over and maintains full operational capability. System adapts to attack manually (e.g., manual transfer to a pre-planned configuration).
Low Protections may not be fully effective against attacks. Attack evades detection. System **or** operators unable to respond to attacks. Some defensive (physical **or** logical) measures are in-place on target system.	**Low** System cannot anticipate the threat but operator can change the attack surface to a degraded alternate capability within its enclave. Architecture consists of computing assets that cannot withstand attacks. System partially recovers but does not maintain full operational capability. System adapts to attack manually (e.g., locking-out all users).
Very Low Protections are ineffective or not implemented against attacks. Attack evades even sophisticated detection. System **or** operators unable to respond to attacks. No defensive (physical **or** logical) measures are in-place on target system.	**Very Low S**ystem cannot anticipate the threat and operator unable to change the attack surface. System cannot withstand an attack. System cannot recover from an attack to maintain operational capability .System cannot adapt to an attack.

Matrix (Scale derived from Industry Best Practices Paper)		Resiliency				
		Very High	High	Moderate	Low	Very Low
Effectiveness of Defense	Very Low	Low	Moderate	High	Very High	Very High
	Low	Low	Moderate	Moderate	High	Very High
	Moderate	Low	Low	Moderate	Moderate	High
	High	Very Low	Low	Low	Moderate	Moderate
	Very High	Very Low	Very Low	Low	Low	Low

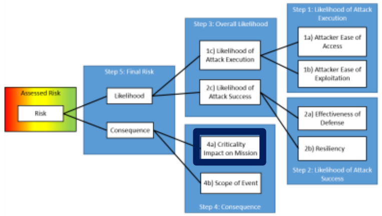
Step 3: Determining Likelihood

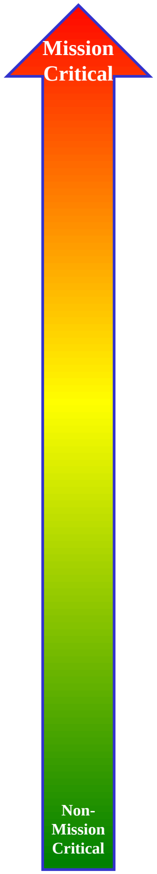

Assessed Risk
Risk
Step 5: Final Risk
Likelihood
Consequence
Step 3: Overall Likelihood
1c) Likelihood of Attack Execution
2c) Likelihood of Attack Success
Step 1: Likelihood of Attack Execution
1a) Attacker Ease of Access
1b) Attacker Ease of Exploitation
2a) Effectiveness of Defense
2b) Resiliency
Step 2: Likelihood of Attack Success
4a) Criticality Impact on Mission
4b) Scope of Event
Step 4: Consequence

- **Take results of Step 1 Likelihood of Execution, and place on Y-Axis**
  - **Likelihood of Attack Execution is <u>{insert Level}</u>**
- **Take results of Step 2 Likelihood of Success and place on X-Axis**
  - **Likelihood of Attack Success is <u>{insert Level}</u>**
- **Result is your Final Likelihood**
  - **Final Likelihood is <u>{insert Level}</u>**

Matrix (Scale derived from NIST 800-30r1)		**Likelihood of Attack Success**				
		Very Low	**Low**	**Moderate**	**High**	**Very High**
Likelihood of Attack Execution	**Very High**	Low	Moderate	High	Very High	Very High
	High	Low	Moderate	Moderate	High	Very High
	Moderate	Low	Low	Moderate	Moderate	High
	Low	Very Low	Low	Low	Moderate	Moderate
	Very Low	Very Low	Very Low	Low	Low	Low

Step 4a: Criticality Impact on Mission (Determining Consequence)


Assessed Risk
Risk
Step 5: Final Risk
Likelihood
Consequence
Step 3: Overall Likelihood
1c) Likelihood of Attack Execution
2c) Likelihood of Attack Success
4a) Criticality Impact on Mission
4b) Scope of Event
Step 4: Consequence
Step 1: Likelihood of Attack Execution
1a) Attacker Ease of Access
1b) Attacker Ease of Exploitation
2a) Effectiveness of Defense
2b) Resiliency
Step 2: Likelihood of Attack Success



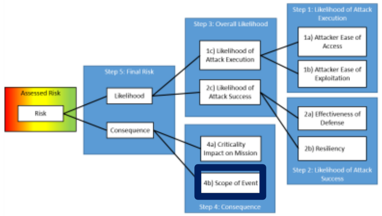
CRITICALITY IMPACT ON MISSION
Very High Mission-critical information system supporting successful long haul flight, drone release and package delivery. Established priorities and values of high-value assets related to identifying target. Operations and sustainment related to, but not limited to, wide body aircraft, delivery drones, Widget Deliveries mission network, & package delivery sensors.
High Mission Support information systems needed to support launch activities, but not critical. Operations and sustainment related to, but not limited to, Widget Deliveries airfield operations, Widget Deliveries Super Secure Vault (SSV) assembly area (SAA), & drone maintenance control system (DMCS).
Moderate Test Support Systems are only used during testing. Operations and sustainment of systems related to, but not limited to, Drone Emulation and Simulation System (DESS), Warehouse Simulation Framework (WSF), & Customer Event Simulator (CES).
Low Training and Secondary Security support information systems used for operator training and monitoring of physical security systems. Operations and sustainment of systems related to, but not limited to, Worldwide Super Secure Ops Module (WSSOM), Drone Safety Awareness System (DSAS), Widget Drones test network environment (WDTNE), & Widget Drones CEO Dashboard (WDCO).
Very Low Ancillary Support information systems used as maintenance equipment of supporting functions. Operations and sustainment of systems related to, but not limited to, AV Laptop, & Vulnerability Scanning Systems (VSS).

Criticality Impact on Mission is intended to characterize the criticality of the system targeted by the attack under analysis towards the Widget Deliveries mission. This is a characterization of the mission of the specific system targeted, with expected values corresponding to the system’s role in the Widget Deliveries mission.

Results for Criticality Impact on Mission is {Insert Level}

- Justification for determined consequence needs to be specific to the system being assessed

Step 4b: Scope of Event (Determining Consequence)


Assessed Risk
Risk
Step 5: Final Risk
Likelihood
Consequence
Step 3: Overall Likelihood
1c) Likelihood of Attack Execution
2c) Likelihood of Attack Success
Step 4: Consequence
4a) Criticality Impact on Mission
4b) Scope of Event
Step 1: Likelihood of Attack Execution
1a) Attacker Ease of Access
1b) Attacker Ease of Exploitation
Step 2: Likelihood of Attack Success
2a) Effectiveness of Defense
2b) Resiliency

Scope of Event is intended to characterize the expected impact to the targeted system's primary functions based on a successful execution of the attack under analysis. This includes any direct adverse effects caused (e.g. destruction of equipment or potential loss of life), impact to the mission of the systems (e.g. primary mission function disrupted vs. primary mission function diminished to an extent), and any exposure across the broader Widget Deliveries system caused by the exploitation (e.g. all systems exposed across the Widget Deliveries enterprise vs. effects that can be contained).

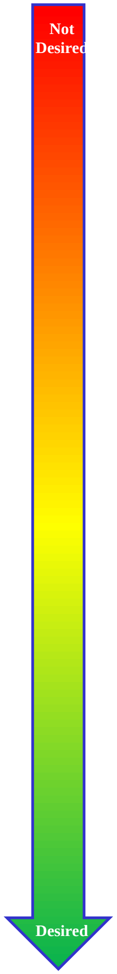
Within the Scope Criteria, select the attribute level for each of the following:

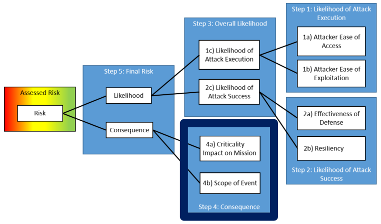
1. Exposure
2. Impact

Results for Scope Criteria is {Insert Level}

- Justification for determined consequence needs to be specific to the system being assessed

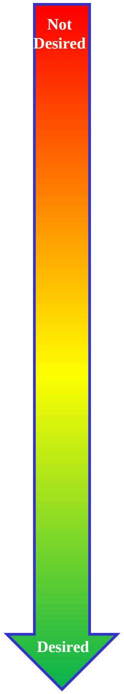
SCOPE CRITERIA
Very High 1. All systems are fully exposed across all sites, and effects cannot be contained (i.e., no systems available). 2. Assessed Threat Event causes multiple severe or catastrophic adverse effects.
High 1. Broad exposure across multiple sites, and effects cannot be contained (i.e., more than one site unavailable). 2. Assessed Threat Event causes serious degradation, disruption or loss of ability to perform primary function.
Moderate 1. Moderate exposure across the sites, and effects may or may not be contained (i.e., entire site is unavailable). 2. Assessed Threat Event causes significant degradation or disruption, and ability to perform primary functions is significantly reduced.
Low 1. Limited exposure across the sites, and effects can be contained (i.e., a system within a system is unavailable). 2. Assessed Threat Event causes limited degradation, and ability to perform primary function is diminished to an extent and not noticeably reduced.
Very Low 1. No exposure across the sites, and effects are isolated or non-existent (i.e., only one server affected). 2. Assessed Threat Event causes negligible adverse effect on ability to perform primary function.



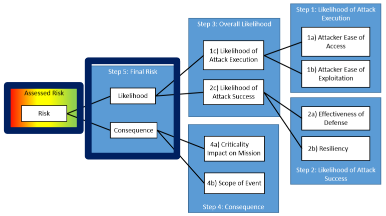

Step 1: Likelihood of Attack Execution
1a) Attacker Ease of Access
1b) Attacker Ease of Exploitation
Step 3: Overall Likelihood
1c) Likelihood of Attack Execution
2c) Likelihood of Attack Success
Step 5: Final Risk
Likelihood
Consequence
Assessed Risk
Risk
4a) Criticality Impact on Mission
4b) Scope of Event
Step 4: Consequence
2a) Effectiveness of Defense
2b) Resiliency
Step 2: Likelihood of Attack Success

Step 4c: Determining Consequence

CRITICALITY IMPACT ON MISSION	SCOPE CRITERIA
Very High Mission-critical information system supporting successful engagement, tactical and flight test. Established priorities and values of high-value assets related to identifying target. Operations and sustainment related to, wide body aircraft, delivery drones, Widget Deliveries mission network, & package delivery sensors.	**Very High** All systems are fully exposed across all sites, and effects cannot be contained (i.e., no systems available). Assessed Threat Event causes multiple severe or catastrophic adverse effects.
High Mission Support information systems needed to support launch activities, but not critical. Operations and sustainment related to, but not limited to, Widget Deliveries airfield operations, SAA, & DMCS.	**High** Broad exposure across multiple sites, and effects cannot be contained (i.e., more than one site unavailable). Assessed Threat Event causes serious degradation, disruption or loss of ability to perform primary function.
Moderate Flight/Ground Test Support Systems are only used during test mission. Operations and sustainment of systems related to, but not limited to, DESS, WSF, & CES.	**Moderate** Moderate exposure across the sites, and effects may or may not be contained (i.e., entire site is unavailable). Assessed Threat Event causes significant degradation or disruption, and ability to perform primary functions is significantly reduced.
Low Training and Secondary Security support information systems used for warfighter training and monitoring of physical security systems. Operations and sustainment of systems related to, but not limited to, WSSOM, DSAS, WDTNE, & WDCO.	**Low** Limited exposure across the sites, and effects can be contained (i.e., a system within a system is unavailable). Assessed Threat Event causes limited degradation, and ability to perform primary function is diminished to an extent and not noticeably reduced.
Very Low Ancillary Support information systems used as maintenance equipment of supporting functions. Operations and sustainment of systems related to, but not limited to, AV Laptop, & VSS.	**Very Low** No exposure across the sites, and effects are isolated or non-existent (i.e., only one server affected). Assessed Threat Event causes negligible adverse effect on ability to perform primary function.



Matrix (Scale derived from NIST 800-30r1)		Scope				
		Very Low	**Low**	**Moderate**	**High**	**Very High**
Criticality Impact on Mission	**Very High**	Low	Moderate	High	Very High	Very High
	High	Low	Moderate	Moderate	High	Very High
	Moderate	Low	Low	Moderate	Moderate	High
	Low	Very Low	Low	Low	Moderate	Moderate
	Very Low	Very Low	Very Low	Low	Low	Low


Assessed Risk
Risk
Step 5: Final Risk
Likelihood
Consequence
Step 3: Overall Likelihood
1c) Likelihood of Attack Execution
2c) Likelihood of Attack Success
Step 4: Consequence
4a) Criticality Impact on Mission
4b) Scope of Event
Step 1: Likelihood of Attack Execution
1a) Attacker Ease of Access
1b) Attacker Ease of Exploitation
Step 2: Likelihood of Attack Success
2a) Effectiveness of Defense
2b) Resiliency

Step 5: Determining Final Risk

- **Take results of Step 3: Determining Likelihood and place on Y-Axis**
  - **Likelihood is <u>{insert Level}</u>**
- **Take results of Step 4: Determining Consequence and place on X-Axis**
  - **Consequence is <u>{insert Level}</u>**
- **Result is your Final Risk Determination**
  - **Final Risk is <u>{insert Level}</u>**

Matrix (Scale derived from Widget Deliveries Risk Management Plan)		Consequence				
		Very Low (1)	Low (2)	Moderate (3)	High (4)	Very High (5)
Likelihood	Very High (5)	Low	Moderate	High	Very High	Very High
	High (4)	Low	Moderate	Moderate	High	Very High
	Moderate (3)	Low	Low	Moderate	Moderate	High
	Low (2)	Very Low	Low	Low	Moderate	Moderate
	Very Low (1)	Very Low	Very Low	Low	Low	Moderate

Cyber Risk Board Authorities/Responsibilities

- **Tier 1 (CEO chair):**
  - **Baseline all organization/company level risks**

- **Tier 2 (CTO chair):**
  - **Baseline moderate, high, or very high (yellow or red) risks**
  - **Submit company level risks to CEO**
  - **Provide summary of high and very high risks to Tier 1 board to provide situational awareness**

- **Tier 3 (Cybersecurity Division Chief chair):**
  - **Baseline low (green) risks**
  - **Provide summary of all risks adjudicated at Tier 3 board to Tier 2 board to provide situational awareness**

Risk Presentation Format
(company proprietary when filled in)

Risk Summary

CONDITION:

[What is known today]

IF:

[The specific risk event under evaluation]

THEN:

[The consequence to the product, business service, or company from a mission delivery perspective if the risk is realized, or set of consequences, that will impact the system/program/activity if the risk event occurs.]

RATIONALE FOR RISK ASSESSMENT:

[Short summary of salient points of why risk was scored as it was for likelihood and consequence]

Risk Assessment

		Consequence				
		Very Low (1)	Low (2)	Moderate (3)	High (4)	Very High (5)
Likelihood	Very High (5)	Low	Moderate	High	Very High	Very High
	High (4)	Low	Moderate	Moderate	High	Very High
	Moderate (3)	Low	Low	Moderate	Moderate	High
	Low (2)	Very Low	Low	Low	Moderate	Moderate
	Very Low (1)	Very Low	Very Low	Low	Low	Moderate

(Proposed) Mitigation Plan

Mitigation Steps	Completed? (Y/N)	(Projected) Date
1. …		
2. …		
3. …		
Etc.		
Responsible Office for Remediation: *(product or business unit manager)*		
Assigned Priority for Remediation: *X of Y Open Risks*		

Conclusion

Assumptions:

Pre-Conditions Used:

Board Recommended Actions:

Additional Notes/Uncertainties:

Summary

- **Widget Deliveries Cybersecurity Risk Assessment Methodology implemented**
  - **Developed with key stakeholders**
  - **Traceable to applicable laws**
  - **Employs NIST 800-30r1 & industry best practices methodology which simplifies assessment feasibly reducing subjectivity of responses**
  - **Cyber risks stored with restricted access**
  - **Process will be reviewed (at least annually)**