Baseline Development for ICT Supply Chain Assessments

DCIO/CS Risk Assessment & Operational Integration

This Page Intentionally Blank

Baseline Development for ICT Supply Chain Assessments

This document is still undergoing review and is subject to modification or withdrawal.

Any reference in other publications should appropriately caveat the draft nature of this document.

This document, is one of multiple guides, and processes, developed for the Deputy DoD CIO for Cybersecurity's Director for Risk Assessment and Operational Integration (RA&OI) under IDA Project BC-5 4771, in support of ongoing DoD CIO efforts to manage supply chain risks in acquiring and using Cyber and Information and Communications Technology (ICT).

The Director, RA&OI believes that these documents, while developed individually for specific analytical purposes, can provide insight to the DoD community as examples for assessing Cyber and ICT supply chain risk.

IDA

INSTITUTE FOR DEFENSE ANALYSES
730 EAST GLEBE ROAD
ALEXANDRIA, VIRGINIA 22305

Acknowledgements

Three Sixty Corporation, Chris Garvin

Gregory N. Larsen, *Task Leader*
Ken Hong Fong, *Project Leader*
Reginald M. Meeson, Jr.

Baseline Development for ICT Supply Chain Assessments

Version 1.0
2/3/2022

This Guide was developed by the Three Sixty Corporation for their use in conducting supply chain risk assessments for their federal customers, and adapted and released for DoD community information, under IDA Project BC-5-4771, as an optional process and format for conducting cyber-related vendor supply chain reviews. This methodology can be further tailored to specific organizational and mission needs. It is intended to guide the identification, assembly, and analysis of essential elements of information that the Three Sixty Corporation had found useful for their sponsors decision making. DoD organizations can add, tailor, or exclude sections not germane to their analysis.

Contents

Purpose:
This ICT Supply Chain Assessment is a multi-step process describing steps to research and analyze company information. It provides guidance to non-counterintelligence trained personnel (80%) allowing them to conduct a supply chain risk assessment by applying analysis and judgement to publicly available information (PAI) on a company (vendor, supplier, manufacturer…). This allows the relationships among the operational and mission variables to be determined and facilitates risk-based decision making and identification of whether counterintelligence personnel (20%) should be consulted.

Scope:
The intended use is for decision makers and supply chain risk management (SCRM) teams, as guidance for analyzing company information and evaluating supply chain risk.

Roles and Responsibilities:

Risk Owner
Responsibilities

- Decision maker

SCRM Team
Responsibilities

- Advisory services and subject matter expertise
- Centralized hub for awareness
- Liaison to external stakeholders
- Information sharing management

Researcher
Responsibilities

- Complete the Supply Chain Risk Assessment (SCRA) table
- Complete the SCRA worksheet
- Report findings

Introduction to the Company Overview:
A company overview presents PAI on a company and its products and services in a consistent and uniform manner. The company overview provides the 80% with a structured template for compiling information used in conducting a SCRA.

An overview consists of segments on business structure, financial, lineage, legal, supply chain, and cybersecurity information.

A company overview is produced by completing the company overview template. The company overview itself is not a risk assessment and will not include risk scores and conclusions, allowing the information to be shared with limited restrictions.

The following bullets outline information that is provided in a company overview.

- ***Business Structure Information***
  Country of origin of company, registrations, and company structure.
- ***Financial Information***
  Identified revenue, government contracts, market share, and financial issues.

- ***Company Lineage Information***
  Historical mergers and acquisitions.
- ***Legal Information***
  Identified legal cases that would hinder a company's ability to perform on a contract.
- ***Supply Chain Information***
  Identified research and development (R&D), manufacturing, testing, quality control, and storage locations.
- ***Cybersecurity Information***
  Known vulnerabilities, breaches, and responses.

Company Overview Template:

The company overview template is a structured set of data fields that ensure information is compiled and presented in a consistent and uniform manner.

Company Name Address of Corporate HQ			
Parent	*https://sam.gov/content/entity-information*	**Parent Country**	*Parent company website*
DUNS	*https://sam.gov/content/entity-information* and *https://www.dnb.com/duns-number/lookup.html*	**CAGE Code**	*https://sam.gov/content/entity-information* and *Commercial and Government Entity Program (dla.mil)*
Holding Type	**Public or Private** *Company website*	**Date Founded**	*https://sam.gov/content/entity-information*
Incorporated In	**State** *https://sam.gov/content/entity-information*	**Company Website**	*Company website*
Entity Status	**State Registration: Active / Inactive** *State's Corporation Commission business entity search*	**SAM: Active/Inactive/Excluded** *https://sam.gov/content/entity-information*	**SBA: Designation (SDVOSB, WOSB, 8A...)** *https://sam.gov/content/entity-information*
Foreign Ownership	*Company website / press release / SEC fillings*	**Workforce**	*Web search for employee count and employment history websites*
Revenue and Financial Health *https://www.usaspending.gov/search - for USG contract information* *https://www.sec.gov/edgar/search/ – For public companies' annual revenues*			
USG Prime Contracts	**USG Subcontracts**	**Total Government Dollars Awarded**	**Annual Revenues**
2022:	**2022:**	**2022:**	**2022:**
2021:	**2021:**	**2021:**	**2021:**
2020:	**2020:**	**2020:**	**2020:**
2019:	**2019:**	**2019:**	**2019:**
2018:	**2018:**	**2018:**	**2018:**

Private Sector Clients & Partnerships *www.companywebsite/clients* *https://www.usaspending.gov/search -subcontract details*	
1.	2.
3.	4.

Joint Venture(s)	*Web search / company press releases*
Merger(s)	*Web search / company press releases*
Acquisition(s)	*Web search / company press releases*

Significant Legal Cases *Web search (websites that compile and sort legal cases)*			
Case Type		**Date**	
Background			
Verdict			

Miscellaneous	
Q/A Certifications	*1. Company website*
	2. https://stage.cmmiinstitute.com/learning/appraisals/results
	3. https://www.iso.org/
Foreign Offices Locations	*Company website / website showing employment history*
Victim of Cyber Breach	*Web search (sites that cover cyber news)*
Victim of Insider Breach	*Web search (sites that cover cyber news)*

Development, Storage, and Manufacturing Locations *Company career page / company privacy statements / websites showing employment history / US Import data sites*	
Name	**Location**
1.	
2.	

Known Suppliers *US Import data sites*	
Name	**Location**
1.	
2.	

Product Inventory *https://nvd.nist.gov/search*			
Product Name			
Model #		**CVEs in NIST NVD**	
Unpatched CVEs		**CVSS Score for Unpatched CVEs**	
Product Name			
Model #		**CVEs in NIST NVD**	
Unpatched CVEs		**CVSS Score for Unpatched CVEs**	

Introduction to the Company Overview Worksheet:

The company overview worksheet facilitates a structured way of processing company overview information aiding in the production of SCRAs to a consistent quality standard.

The worksheet provides step by step instructions on how to process information compiled within a company overview and aids in the determination of supply chain risks.

Steps to process a Company Overview:

1. Complete the company overview template, by following the URLs in each field, using other available publicly available information, or using information from data providers. Ensure to cite all information included in the company overview template.

2. Fill out the section of the company overview worksheet that identifies the name of the company and products being scored, using information from the company overview template. Reference Appendix A-E within this guide for more detailed information on how to complete the worksheet.

3. Complete the section on Supply Chain, Business Structure, and Company Lineage Likelihood and Impact Scoring by pulling information from the relevant company overview section. Reference Appendix A for more details on how to complete the worksheet.

4. If the company overview has identified any foreign ownership, control, or influence (FOCI) concerns then calculate an Impact score using the worksheet and the Threat Information Sheet (TIS). An example of a TIS can be found in Appendix B.

5. Complete the cyber information scoring section of the worksheet referencing any vulnerabilities identified in the company overview. Reference Appendix C of this guide for additional resources needed to conduct research on the vulnerabilities. Cyber information scoring may require additional subject matter expertise.

6. Complete the financial section of the of the worksheet using data from the company overview. Reference Appendix D for details. Financial information scoring may require input from the risk owner.

7. Conduct the legal information scoring section of the worksheet using data from the company overview. Reference Appendix E for details. Financial information scoring may require input from the risk owner.

8. Upon scoring each section, input the scores into the heat map and log the findings in the risk tracker.

9. Retain the completed worksheet in accordance with record keeping procedures.

Appendix A: Supply Chain, Business Structure, and Company Lineage Likelihood and Impact Scoring

This appendix describes the process followed for scoring human threat sources that are likely to have an interest in exploiting attack vectors within the supply chain being assessed. Threat sources are characterized and presented in the threat source tables. The threat source table, the geolocation likelihood table, and threat impact table are used to determine the likelihood and impact of a risk.

A threat source is any entity with means, motivation and intent to exploit an attack vector.

The definitions of threat, threat source, and vulnerability are derived from National Institute of Standards and Technology Special Publication (NIST SP) 800-30 and the Committee on National Systems Security (CNSS) Instruction No. 4009.

Likelihood of Geolocation Risks:
Company overviews that identify any foreign-based operations and do not have identified foreign ownership, control, or influence (FOCI) concerns shall be scored against a fixed set of criteria to determine the likelihood of any identified Geolocation Risks. In order to determine whether geolocation risks exist, search for evidence of the following scenarios in the company overview which would indicate a concern:

Is the company, or its parent entity, headquartered in a foreign country?
For hardware or physical products: Are any reviewed products or components of reviewed products that can present espionage or sabotage concerns designed, manufactured, tested, certified, or stored in a foreign country?
For software or digital products: Are any reviewed programs developed, quality assurance tested, localized, certified, maintained, or either supported or hosted by servers located in a foreign country?
For services: Are any reviewed services that can present espionage or sabotage risks conducted by individuals or automated programs based or hosted in a foreign country?
If any of the above-mentioned scenarios are true, then Geolocation Risks exist, necessitating further evaluation to determine risk severity and the likelihood of such risks. To determine risk likelihood, evaluate the Geolocation Risk likelihood indicators captured in Table 1 and referencing Appendix B, and assigns a score (yes = 1, no = 0) to each.

Table 1: Geolocation Likelihood Criteria

Likelihood Level	Geolocation Risk Indicators
Yes (1) / No (0)	Are company operations located in a foreign country listed in any Appropriations Act, Executive Orders, or other applicable policies?
Yes (1) / No (0)	Are company operations located in a foreign country with laws that allow the government to influence and / or collect on companies operating in their territory?
Yes (1) / No (0)	Are company operations located in a foreign country with a known or documented history of conducting cyber espionage (CE) or sabotage campaigns against other state or non-state actors?
Yes (1) / No (0)	Are company operations located in a foreign country that has a history of influencing or forcing companies to provide access to company intellectual property such as source code, patents, designs, etc., that would be relevant to the reviewed product(s)?

Yes (1) / No (0)	Is any of the company's leadership or ownership politically exposed to the country or connected to the country's government in which it is operating?

**The sum of the scores is tallied to determine an overall numerical likelihood value. The overall value likelihood categorizations correlate with the risk level displayed in a heat map, which range from 1-5, with 5 being the highest likelihood rating.*

Table 2: Geolocation Likelihood Scoring Table

Geolocation Characteristics					
Nation State	**Policy/App Act**	**Country's Laws**	**Cyber Espionage History**	**Country's History**	**FOCI**
Name of Country	1 or 0	1 or 0	1 or 0	1 or 0	1 or 0

If Company or any leadership shows ties to a foreign country's government, military, or intelligence service, then use threat source information to determine impact.

Table 3: Threat Source Impact Scoring Table

Threat Source Characteristics					
			Motivation		
Threat Source	**Technical Capability**	**Funding Capability**	**Peacetime Scenario**	**Crisis Scenario**	**Intent**
Name of Nation State	Yes=1 or No=0	1 or 0	1 or 0	1 or 0	1 or 0

**The sum of the scores is tallied to determine an overall numerical impact value. The overall value impact categorizations correlate with the risk level displayed a heat map, which range from 1-5, with 5 being the highest impact rating.*

Technical and Funding Capability:

Technical capabilities are characterized by a documented understanding of the technology resources that are currently available to the threat source, the research and development capabilities, the expected and documented levels of technical expertise and personnel, training, and observed actions that demonstrate a level of technical competence.

Funding capabilities are characterized by a documented understanding of the wealth resources of a nation state or non-state actor. It is focused on a documented understanding of their priorities for allocating funds towards the execution of attack activities, towards research and development of attack related tools and techniques, and the degree to which funding is allocated to technical training related to cyber warfare and associated technologies. The determination of funding capabilities can also consider known alliances and agreements for funding assistance between nation states and between nation states and non-state actors (APTs/organized crime).

Table 4: Technical and Funding Capability

Value	**Description**
	Technical Capability to Skill Required for Exploit = Technical Requirement
1	The Threat Source technical capabilities meet the vulnerability exploitation skill requirements.
0	The Threat Source technical capabilities do not meet the vulnerability exploitation skill requirements.
	Funding Capability to Expense of Exploit = Funding Expense
1	The Threat Source funding capabilities meet the vulnerability exploitation funding requirements.

0	The Threat Source funding capabilities do not meet the vulnerability exploitation funding requirements.

Motive / Goals / Objectives:

Motive is characterized by an understanding of the rationale that could drive a threat source to execute a threat action.

Table 5: Motivations

Motivation	Goals / Objectives
Political Advantage	Change world opinion or force changes in policies / seek negotiation advantage
	Ridicule / embarrass an adversary
Military Advantage	Intelligence collection (steal data, map environment) / Disrupt services prior to, or during, an attack
	Inject misinformation or cause denial of services / Gain access
	Gain control / Destroy information
	Test strength of defenses (as prelude to an attack)
Social	Instigate change – change way of life
Issue oriented	Protect something believed to be important
	Prove a point (e.g., cause damage to prove the need of a mitigation)
Religious / Ideological	Rid the world of a perceived evil
Economic	Financial gain
	Inflict financial damage

Reference Appendix B to determine if a Threat Source has demonstrated motives.

Evidence of Intent:

Intent that a threat source has towards executing some form of an attack is determined by analysis of the threat source's reported statements, as well as any observed and reported attack-related activities by the threat source.

- Stated intent
- Reported threats
- Reported activity
- Reported attempts to develop the means for an exploit
- Reported types and numbers of actual attack attempts

Reference Appendix B to determine if a Threat Source has documented evidence of intent.

Appendix B: Example of a Threat Information Sheet (TIS)

	Country Cyber Threat Information
1	Often uses high-volume attacks with large number of operatives in military or outside groups linked to government who bombard targets. Has ability to cause damage in attacks but isn't known to have done so.
	Suspected acts:
	2009: Theft of data from Google Inc. and other tech companies.
	2009: Discovery of theft of plans for U.S. Joint Strike Fighter project.
	2010: Attacks on British executives.
	2011: Attack on South Korean Internet portal.
	2013: Major U.S. media companies hacked.
	2015: "Great Cannon" directs massive amounts of traffic to take anticensorship websites offline.
	2015: Hack of U.S. Office of Personnel Management.
	Malware includes: Hydraq, found in Google attack and others; Sakula, found in OPM attack and others
	Purpose of attack: Surveillance, defacement
	Suspected offensive teams: Military or intelligence, private groups
	Targets: Domestic, international
	Software: Developed in country
	Government comment: "Country X advocates the building of a peaceful, secure, open and cooperative cyberspace, opposes militarization of cyberspace or cyber arms race. The Chinese government staunchly upholds cybersecurity, firmly opposes and combats all forms of cyberattacks in accordance with law."
	Policies: Country X is named in multiple appropriation acts as an entity of concern.

Appendix C: Cyber Information Processing and Scoring

The vulnerability analysis identifies and characterizes system and architecture security weaknesses based on findings associated with the use of the ICTS components under review. A complete vulnerability analysis includes a description of identified vulnerabilities, the accessibility requirements in order to reach and exploit identified vulnerabilities, and the impact of an exploitation. Exploitation impact results communicate the effects on the confidentiality, integrity, and availability of information on the system in question.

Vulnerability tracker:

No.	Vulnerability	Likelihood	Impact	Level
1	CVE 12345.23	Completed in Step 5	-	-
2				
3				

Step 1: Research the Vulnerabilities

Group vulnerability findings and address their root cause. Group vulnerability findings that have a common root cause. Document the findings but address them at their root cause level and include the root cause issue as the weakness that will be exploited.

Address the individual vulnerability finding. Document the specific vulnerability finding and include it in the vulnerability analysis process of the risk assessment for full characterization.

Research and Validate Vulnerability Findings. Resources used to research vulnerabilities may include, but are not limited to:

- Vulnerability databases and alerts, for example:
  - National Vulnerability Database (NVD) (http://nvd.nist.gov/)
  - United States Computer Emergency Readiness Team (US-CERT), Vulnerability Notes Database (http://www.kb.cert.org/vuls)
  - MITRE Corporation's Common Vulnerabilities and Exposures (CVE) List (http://cve.mitre.org/)
  - The Open-Source Vulnerability Database (OSVDB) (http://osvdb.org/)
  - Information Assurance Vulnerability Alert (IAVA) Notifications. The US Cyber Command (https://www.cybercom.mil/) sends out IAVA notifications.
- Hardware and software vendor security alerts and patch notifications.

Step 2: Think Through an Attack

Vulnerability: "Enter a brief descriptive title of the vulnerability"
Description: Provide a brief description of the known security weakness and describe its cause. Explain how it was determined to be a potential security weakness relevant to the target environment. Cite the reference.

<table>
<tr><td colspan="2">**Accessibility Requirements (Access Vector):** Describe the type of access that is required in order to reach and exploit the vulnerability. This should be just a simple explanation of one of the following:
• **Local Network / Host** – The exploit requires local access to the vulnerable component (cannot be reached remotely).
• **External / Remote** – The exploit can be conducted remotely (implies that an insider can also conduct the attack). This can also include remote injection of malicious code that can be activated to conduct any number of different attacks locally.
• **Supply chain** – The exploit requires access to the product’s supply chain.</td></tr>
<tr><td colspan="2">**Exploitation method (Attack Process):** Define requirements in terms of skill level and tools. Describe the financial resource requirements. This information will correlate back to threat source capability.
• **Skill Level Required:** (High, Moderate, or Low)
Describe the technology and skill requirements for exploiting the vulnerability.
Briefly describe the technical / procedural execution requirements for exploiting the vulnerability.
• **Exploit Expense Level:** (High, Moderate, or Low)
Describe the financial resources that may be needed to develop, purchase, and execute the tools and techniques needed to exploit the vulnerability.</td></tr>
<tr><td rowspan="3">**Potential Exploit Results:** Use the Confidentiality, Integrity and Availability spaces to describe the expected technical outcome of a threat action on this vulnerability.</td><td>**Confidentiality** – Explain how an exploit of this vulnerability could impact confidentiality. (Example: could it allow an attacker to access an information resource or to collect data from traffic?)</td></tr>
<tr><td>**Integrity** – Explain how an exploit of this vulnerability could impact integrity. (Example: could it allow an attacker to modify or delete system or mission data in transit or at rest?)</td></tr>
<tr><td>**Availability** – Explain how an exploit of this vulnerability could impact availability. (Example: could it allow an attacker to prevent access temporarily or permanently to a critical resource?)</td></tr>
</table>

Step 3: Determine the Likelihood of the Vulnerabilities being Exploited

Identify existing safeguards and make a determination of their protective, detective, and corrective capabilities when determining the likelihood value for each Cyber Vulnerability risk.

Likelihood of Occurrence	Description
5 – Highly Probable	Technical failure or accident is almost certain to occur.
4 – Probable	Technical failure or accident is highly likely to occur.
3 – Occasional	Technical failure or accident is somewhat likely to occur.
2 – Remote	Technical failure or accident is unlikely to occur.
1 – Improbable	Technical failure or accident is highly unlikely to occur.

Step 4: Determine the Impact if the Vulnerability is Exploited

Mission Impact	Description
5 – Critical	May result in a critical loss of confidentiality, integrity, or availability resulting in an inability to perform one or more critical mission operations due to one or more of the following: • A complete compromise of mission information or services; • Complete destruction or modification of mission information; • Complete destruction or modification of system data; or • An extended system outage or permanent denial of service, causing operations to resume in a hot site environment.
4 – Major	May result in a major loss of confidentiality, integrity, or availability resulting in an adverse effect on mission operations due to one or more of the following: • A compromise of large amounts of mission information or services; • A major loss in stakeholder confidence that one or more of a system's components can perform its functions; • A major destruction or modification of mission information; • A major destruction or modification of system data; or • Considerable system outage, and / or loss of connected stakeholders.
3 – Damaging	May result in a serious loss of confidentiality, integrity, or availability resulting in an adverse effect on mission operations due to one or more of the following: • A compromise of small amounts of mission information or services; • A notable loss of stakeholder confidence in the system's resources or services; • A partial destruction or modification of mission information; • A partial destruction or modification of system data; or • Short-term system outage, and / or loss of connected stakeholders.
2 – Minimal	May result in minor effect on the confidentiality, integrity, or availability of mission operations due to one or more of the following: • No compromise of mission information or services; • A degradation in the effectiveness or efficiency of support services; • A minor loss of stakeholder confidence in the system's resources or services; • A recoverable loss of mission information; • A recoverable loss of system data; or • A short-term loss of connected stakeholders.
1 - Insignificant	The impact to confidentiality, integrity, or availability is negligible. There is no mission impact if the threat source successfully exploits this vulnerability.

Step 5: Record the likelihood and impact score in the tracker

No.	Vulnerability	Likelihood	Impact	Level
1	CVE 12345.23	1-5	1-5	L/M/H

Appendix D: Financial

Consider the provider's current financial state and their capability to meet requirements with current and increased demand. Review the financial background of the company (provider) and consider the impact to the United States Government (USG) should the provider no longer be capable of fulfilling requirements.

- Is the company financially stable?
- Is the company subsidized by a foreign government?
    - Do foreign governments or state-owned enterprises own any significant stakes of the provider?
    - Are there stipulations with regards to government funding?
- Will the company remain viable if their funding is reduced?
- Does the company have an erratic financial history?
- Does the company have 3 years of history providing products or services to the USG?

Likelihood Level	Financial Scoring
Yes (0) / No (1)	Is the provider of the product or service financially stable?
Yes (1) / No (0)	Is the provider of the product or service subsidized by or receive most if their revenue from a state-owned enterprise or foreign government? If so, reference appendix A and scoring using the FOCI scoring method.
Yes (0) / No (1)	Will the provider remain viable if their funding is reduced?
Yes (1) / No (0)	Does the provider have an erratic financial history?
Yes (0) / No (1)	Does the provider have three (3) years of past performance providing products and services to the USG?

Financial Likelihood Scoring					
	Financially Stable	**Foreign Subsidized**	**Viable with reduction**	**Erratic History**	**Past Performance**
Name of Company	1 or 0	1 or 0	1 or 0	1 or 0	1 or 0

	Financial Impact Scoring
5 – Critical	• Failure to meet goals • Significant impact to mission • Severe impact to budget (>$???)
4 – Major	• Failure to meet multiple objectives • Major impact to goal or mission • Major impact to budget ($?? up to $??)
3 – Damaging	• Significant impact to multiple objectives • Minor impact to goal or mission • Significant impact to budget ($? Up to $?)
2 – Minimal	• Significant impact to any single objective • No impact to goal or mission • Moderate impact to budget ($?? Up to $$)

1 - Insignificant	• No impact to goals • Minimal impact to budget (<$??)

*_Dollar amounts ($) are determined by risk owner_

Appendix E: Legal

Consider the company's (provider) current legal standing and their capability to meet requirements. Review the legal history of the provider and consider the impact to the USG should the provider no longer be capable of fulfilling requirements.

- Is the provider registered to do business with the USG?
- Is the provider legally in good standing (State)?
- Is the provider legally able to provide services and products to the USG?
  - If provider is not, due to not being registered in GSA SAM, then is a legal provider acting as a value-added reseller (VAR)? If a VAR is involved, then the answer is yes.
  - If the provider is prohibited from doing business with the USG because of an executive order or regulation, then the answer is No. Consult with a contracting officer.
- Does the provider have a history of legal trouble?
- Does the provider have three (3) years of history providing products or services to the USG?

Likelihood Level	Legal Scoring
Yes (0) / No (1)	Is the provider registered to do business with the USG?
Yes (0) / No (1)	Is the provider legally in good standing (State)?
Yes (0) / No (1)	Is the provider legally able to provide services and products to the USG?
Yes (1) / No (0)	Does the provider have a history of legal trouble?
Yes (0) / No (1)	Does the provider have three (3) years of history providing products or services to the USG?

Legal Likelihood Scoring					
	Registered in SAM	Good standing State	Legally able to do business	Legal History	3 years of history
Name of Company	1 or 0	1 or 0	1 or 0	1 or 0	1 or 0

Legal Impact Scoring	
5 – Critical	• Failure to meet goals • Significant impact to mission • Violation of laws or sanctions • Waiver request required • Major corrective action required • Reputation damaged
4 – Major	• Failure to meet multiple objectives • Major impact to goal or mission • Significant corrective action or mitigation required • Reputation diminished but recoverable
3 – Damaging	• Significant impact to multiple objectives • Minor impact to goal or mission • Moderate corrective action or mitigation required • Reputation diminished but recoverable
2 – Minimal	• Significant impact to any single objective • No impact to goal or mission

	- Minimal corrective action or mitigation required - Reputation questioned but easily recovered
1 - Insignificant	- No impact on goals - Minor corrective action or mitigation required.

Appendix F: Heat Map

The heat map is a data visualization tool used to present the company overview worksheet risk scores and shows the magnitude of the score(s) as colors. A score placed in a green box represents **Low** magnitude, a yellow box represents a **Moderate** magnitude, and a red box represents a **High** magnitude.

Upon completion of the worksheet each section's score(s) will be placed in the heat map and the magnitude recorded in the risk tracker.

Example:

Geolocation section has one (1) score of a 3 likelihood and a 1 for impact. Place the country's assigned letter in the box that intersects the 3 on the likelihood axis and the 1 on the impact axis.

Legal Scoring (LS) section has one (1) score of a 5 for likelihood and a 4 for impact. Place the LS 1 in the box that intersects the 5 on the likelihood axis and the 4 on the impact axis.

Example: Heat Map

Impact	**5**	🟨	🟨	🟥	🟥	🟥
	4	🟩	🟨	🟨	🟥	🟥 *LS1*
	3	🟩	🟩	🟨	🟨	🟥
	2	🟩	🟩	🟩	🟨	🟨
	1	🟩	🟩	🟩 *A*	🟩	🟨
		1	**2**	**3**	**4**	**5**

Likelihood

Example: Risk tracker

No.	Risk	Likelihood	Impact	Level
A	*Geolocation – Data stored in Country A*	*3*	*1*	*Low*
LS1	*Legal – fined for unlawful harvesting of data*	*5*	*4*	*High*

Appendix G: Threat Information Worksheet Examples

The following pages provide examples of threat information gleaned from Publicly Available Information (PAI) sources around the world and with respect to countries that may present concerns.

ARGENTINA

Military doctrine calls for offensive and defensive operations. Former U.S. officials say country is in nascent

1 Purpose of attack: Surveillance

Suspected offensive teams: Military or intelligence

Software: Developed in country

AUSTRALIA

Capable of launching destructive digital attacks, former U.S. official says.

Malware includes: Regin, also linked to the U.K. and others

2 Purpose of attack: Surveillance

Suspected offensive teams: Military or intelligence

Targets: Domestic, international

Software: Developed in country, purchased off the shelf

Government comment: Australia “does not publicly discuss intelligence or operational matters.”

AZERBAIJAN

Human-rights groups say experiences of detained activists suggest online activities are monitored. Hacktivists

3 Purpose of attack: Surveillance

Targets: Domestic

Software: Purchased off the shelf

BAHRAIN

International attacks limited to people with Bahraini ties.

Suspected acts:

4 2014: Off-the-shelf surveillance software used to spy on Bahraini activists seeking asylum in U.K.

Purpose of attack: Surveillance

Targets: Domestic, international

Software: Purchased off the shelf

BANGLADESH

Hacktivist groups engage in significant back-and-forth attacks with Indian hackers. Swiss

5 Purpose of attack: Surveillance, defacement

Suspected offensive teams: Private groups

Targets: Domestic, international

Software: Purchased off the shelf

BELARUS

6 Armed forces responsible for “informational confrontation and counteraction” as well as defense and security.

Suspected offensive teams: Military or intelligence

BELGIUM

Purchased off-the-shelf surveillance software.

7 Purpose of attack: Surveillance

Software: Purchased off the shelf

BOSNIA AND HERZEGOVINA

8 Purchased off-the-shelf surveillance software.

Purpose of attack: Surveillance

Software: Purchased off the shelf

BRAZIL

Federal Police were listed as purchasing surveillance software.

9 Purpose of attack: Surveillance

Targets: Domestic

Software: Purchased off the shelf

BULGARIA

10 Server for off-the-shelf surveillance software on network registered to Bulgarian Ministry of State
Purpose of attack: Surveillance
Software: Purchased off the shelf

CANADA

11 Documents revealed by former NSA contractor Edward Snowden indicate country has developed weapons for
Purpose of attack: Surveillance
Suspected offensive teams: Military or intelligence
Targets: Domestic, international
Software: Developed in country

CHILE

12 Police Investigations department confirmed purchase of surveillance software to local media.
Purpose of attack: Surveillance
Targets: Domestic
Software: Purchased off the shelf

CHINA

13 Often uses high-volume attacks with large number of operatives in military or outside groups linked to government who bombard targets. Has ability to cause damage in attacks but isn’t known to have done so.
Suspected acts:
2009: Theft of data from Google Inc. and other tech companies.
2009: Discovery of theft of plans for U.S. Joint Strike Fighter project.
2010: Attacks on British executives.
2011: Attack on South Korean Internet portal.
2013: Major U.S. media companies hacked.
2015: “Great Cannon” directs massive amounts of traffic to take anticensorship websites offline.
2015: Hack of U.S. Office of Personnel Management.
Malware includes: Hydraq, found in Google attack and others; Sakula, found in OPM attack and others
Purpose of attack: Surveillance, defacement
Suspected offensive teams: Military or intelligence, private groups
Targets: Domestic, international
Software: Developed in country
Government comment: “China advocates the building of a peaceful, secure, open and cooperative cyberspace, opposes militarization of cyberspace or cyber arms race. The Chinese government staunchly upholds

COLOMBIA

14 Ministry of National Defence recommends capabilities include warning systems and ability to attack aggressors. Former U.S. official says military tinkers with off-the-shelf malware to suit espionage needs.
Purpose of attack: Surveillance
Suspected offensive teams: Military or intelligence
Targets: Domestic
Software: Developed in country, purchased off the shelf

CYPRUS

15 Off-the-shelf surveillance software used for national security, not clear if foreign or domestic use.
Purpose of attack: Surveillance
Software: Purchased off the shelf
Government comment: Cyprus “respects rule of law…both domestically and internationally. Any surveillance software that may have been acquired by the government is strictly for national security purposes.”

CZECH REPUBLIC

Police confirmed purchase of surveillance hacking software.

Purpose of attack: Surveillance
16 Targets: Domestic
Software: Purchased off the shelf
Government comment: Tools to monitor electronic communication are “solely for the use of special
investigation teams” fighting serious crime, under approval of a judge and in accordance with legislation. “The

DENMARK

Allocates about $10 million a year for “computer-network operations,” including defense and offense, since
17 2013. Media reports in 2015 that $75 million allocated for offensive cybercapabilities through 2017.
Suspected offensive teams: Military or intelligence
Software: Developed in country

ECUADOR

Suspected acts:
2015: Opposition activist reported email and social media were hacked. Leaked government correspondence
with software vendor Hacking Team suggests he was target of government efforts. Media sites reporting on
18 Purpose of attack: Surveillance
Targets: Domestic
Software: Purchased off the shelf
Government comment: “The government of Ecuador has not been involved in any contract that has served to
attack digital outlets nor political targets. All activities that the intelligence agencies in Ecuador undertake are

EGYPT

Human-rights groups cite government for domestic surveillance. Traces of surveillance hacking software found
on opposition computers. “Egyptian Cyber Army” group claims it attacked online propaganda of Islamic State,
19 Purpose of attack: Surveillance
Targets: Domestic
Software: Purchased off the shelf

ESTONIA

Purchased off-the-shelf surveillance software. Volunteer government-sponsored group Cyber Defence
Purpose of attack: Surveillance
20 Software: Purchased off the shelf
Government comment: “Estonia cannot divulge detailed information about its technical capabilities…Estonia
uses all technical, organizational and other means at its disposal, while holding in high regard the personal

ETHIOPIA

International attacks limited to targets with Ethiopian ties.
Suspected acts:
21 2013: Off-the-shelf hacking software tied to Ethiopia found on computers of U.S. and other citizens who wrote
Purpose of attack: Surveillance
Targets: Domestic, international
Software: Purchased off the shelf

FINLAND

Cyber Security Strategy of 2013 says military should have “intelligence as well as cyberattack” and defense
22 Suspected offensive teams: Military or intelligence
Software: Developed in country
Government comment: Current situation is to guarantee “capabilities, intelligence and proactive measures in

FRANCE

Defensive and offensive cybercapabilities a stated priority for military since 2008. More emphasis put on
Suspected acts:
2009-15: “Animal Farm” cyberespionage attacks on governments and others around the world traced to
23 Malware includes: Casper, found in attacks on Syrian targets; Babar, used in Iran, Europe; Dino, found in the

Purpose of attack: Surveillance
Suspected offensive teams: Military or intelligence
Targets: International
Software: Developed in country

GERMANY

Federal Intelligence Service has hacking capabilities for espionage, former U.S. official says. State governments
Suspected acts:
2014: Media reports allege country hacked communications of foreign leaders, including Hillary Clinton when
24 Malware includes: R2D2, found on domestic targets
Purpose of attack: Surveillance
Suspected offensive teams: Military or intelligence
Targets: Domestic, international
Software: Developed in country, purchased off the shelf

HONDURAS

25 Human-rights groups say domestic surveillance conducted, unclear if cybertools used.
Purpose of attack: Surveillance
Software: Purchased off the shelf

HUNGARY

Bureau known for international activities purchased off-the-shelf surveillance software. Unclear if used
26 Purpose of attack: Surveillance
Targets: International
Software: Purchased off the shelf

INDIA

Developing offensive capabilities.
Suspected acts:
2010-13: Relatively unsophisticated "Operation Hangover" espionage attacks around the world, particularly
27 against China and Pakistan, traced to Indian company. The company and Indian government deny
Purpose of attack: Surveillance, defacement
Suspected offensive teams: Military or intelligence, private groups
Targets: International
Software: Developed in country

IRAN

A top country of concern, with destructive capabilities. Iranian media report government claims ability to
Suspected acts:
2012: Computers wrecked at Saudi Aramco.
2013: Denial-of-service attacks against U.S. financial institutions.
28 Malware includes: Shamoon, used against energy-sector targets
Purpose of attack: Surveillance, defacement, destruction
Suspected offensive teams: Military or intelligence, private groups
Targets: Domestic, international
Software: Developed in country

ISRAEL

Unit 8200 cyberspying agency widely considered to be among world's most advanced. Some activities appear
Suspected acts:
2010: Discovery of computer worm that destroyed centrifuges at Iranian nuclear plant.
2015: Spying on the P5+1 talks on Iranian nuclear program.
29 Malware includes: Duqu, earlier version seen in conjunction with Stuxnet, advanced version used in P5+1
hacks; Flame, used in espionage, particularly in preparations for attack on Iran's nuclear program, also linked

Purpose of attack: Surveillance, destruction
Suspected offensive teams: Military or intelligence
Targets: Domestic, international
Software: Developed in country

ITALY

Military has electronic warfare unit, according to U.N.; unclear how advanced. Agencies working
30 Purpose of attack: Surveillance
Suspected offensive teams: Military or intelligence
Targets: Domestic, international
Software: Developed in country, purchased off the shelf

KAZAKHSTAN

Purpose of attack: Surveillance
31 Software: Purchased off the shelf
Government comment: Kazakhstan “supports the U.N. Resolution ‘On Creation of a Global Culture of Cybersecurity’ given that our activities strongly comply with its main principles. In particular, the Government of Kazakhstan recognizes that in a democratic society cybersecurity should be implemented in accordance

LEBANON

Evidence of digital spying on foreign countries. Leaked documents indicate Lebanese officials installed
Suspected acts:
32 2012-15: “Volatile Cedar” attacks on countries in Mideast, U.S. and others linked to Lebanon; blamed by Israel
Malware includes: Explosive, used in “Volatile Cedar”
Purpose of attack: Surveillance
Targets: Domestic, international
Software: Developed in country, purchased off the shelf

LUXEMBOURG

Purchased off-the-shelf surveillance software.
Purpose of attack: Surveillance
Targets: Domestic
Software: Purchased off the shelf
33 Government comment: “Surveillance software was indeed acquired by the Luxembourg Intelligence Service from an Italian firm. The mandate of that service is comparable to the FBI national intelligence mandate. The service does consequently not have activities outside the national territory, nor does it engage in international surveillance operations. The software, which was especially tailored to the needs of the service, was used exclusively for the internal interception of communications, based on the Luxembourg code of criminal procedure, which allows ‘the control and surveillance of all forms of communications by appropriate technical

MALAYSIA

34 Purchased off-the-shelf surveillance software.
Purpose of attack: Surveillance
Software: Purchased off the shelf

MEXICO

Suspected acts:
Ongoing: Hacking tools used to spy on Central American drug cartels.
35 Purpose of attack: Surveillance
Targets: Domestic, international
Software: Purchased off the shelf

MONGOLIA

36 Purchased off-the-shelf surveillance software.
Purpose of attack: Surveillance

Software: Purchased off the shelf

MOROCCO

Hacking software found targeting Moroccan journalists critical of government.
37 Purpose of attack: Surveillance
Targets: Domestic
Software: Purchased off the shelf

MYANMAR

Military Affairs Security has mission of “network-centric warfare” and “cybercapabilities,” according to
Suspected acts:
38 2011: Exile groups reported sites taken down by denial-of-service attacks.
Purpose of attack: Surveillance, defacement
Suspected offensive teams: Military or intelligence
Targets: Domestic, international

NETHERLANDS

Military receives training from Dutch cybersecurity company Fox-IT. Purchased off-the-shelf surveillance
39 Purpose of attack: Surveillance
Suspected offensive teams: Military or intelligence
Software: Developed in country, purchased off the shelf

NEW ZEALAND

Helped U.S. spy on China, according to leaked documents revealed by former NSA contractor Edward
Purpose of attack: Surveillance
40 Suspected offensive teams: Military or intelligence
Targets: International
Software: Developed in country
Government comment: “We don’t comment on speculation about matters that may or may not be

NIGERIA

Attempted to use surveillance software on Nigerian telecoms.
41 Purpose of attack: Surveillance
Targets: Domestic
Software: Purchased off the shelf

NORTH KOREA

South Korean reports peg North Korea’s hacker forces at more than 5,000. Security experts debate
capabilities but say country is of concern because of willingness to use destructive tools. Also known for
Suspected acts:
2013: Discovery of “Kimsuky” espionage attacks on South Korean targets.
42 2014: Destruction and leaking of data at Sony Pictures Entertainment.
Malware includes: Destover, used in Sony attack
Purpose of attack: Surveillance, destruction
Suspected offensive teams: Military or intelligence
Targets: International
Software: Developed in country

NORWAY

Cyber Defense Force acknowledged country was preparing offensive cyberweapons.
Suspected offensive teams: Military or intelligence
43 Software: Developed in country
Government comment: “Norway has chosen a comprehensive approach to coordinate cybersecurity measures
across the ministries of Justice and Public Security, Defense, Transport and Communications as well as

OMAN

44 Purpose of attack: Surveillance
Software: Purchased off the shelf

PAKISTAN

Groups linked to cyberespionage campaigns as well as defacement attacks on Indian targets, in long-running
Suspected acts:
2013: “Operation Arachnophobia” gathered documents from target computers and was designed to look like it
45 Malware includes: Bitterbug, used in espionage
Purpose of attack: Surveillance, defacement
Suspected offensive teams: Private groups
Targets: Domestic, international
Software: Developed in country, purchased off the shelf

PANAMA

Leaked documents indicating purchase of surveillance equipment from vendor Hacking Team ignited a furor,
46 as former president accused of spying on enemies and surveillance equipment reportedly went missing.
Purpose of attack: Surveillance
Targets: Domestic
Software: Purchased off the shelf

PHILIPPINES

Multiple researchers say they have seen malware with ties to the Philippines spread internationally, targeting
47 Purpose of attack: Surveillance
Targets: International
Software: Developed in country

POLAND

Military strategy calls for both defensive and offensive capabilities. Anticorruption bureau purchased products
48 Purpose of attack: Surveillance
Suspected offensive teams: Military or intelligence
Targets: Domestic
Software: Developed in country, purchased off the shelf

QATAR

Officials approached U.S. defense contractors on building offensive capabilities, former U.S. officials say.
49 Purpose of attack: Surveillance
Software: Developed in country, purchased off the shelf

RUSSIA

Known for complex malware, including some that takes instructions from Twitter accounts. Also uses common
techniques such as phishing. Malware also used in criminal activities. Own-developed and off-the-shelf
Suspected acts:
2007: Massive denial-of-service attack on Estonia.
2014: Breach of White House and State Department email systems.
2015: Attacks on Ukrainian military computers.
50 Malware includes: BlackEnergy, used in crime and political espionage; The CozyDuke, MiniDuke, CosmicDuke
Purpose of attack: Surveillance, defacement, destruction
Suspected offensive teams: Military or intelligence, private groups
Targets: Domestic, international
Software: Developed in country, purchased off the shelf
Government comment: “Russia has never waged cyberwarfare against anyone. Russia believes that the
cybersphere should be used exclusively for peaceful purposes. Ideally, our country would like to see the

SAUDI ARABIA

Off-the-shelf mobile-phone malware targets Saudi protesters.

51	Purpose of attack: Surveillance Targets: Domestic Software: Purchased off the shelf
	SINGAPORE
52	Unclear international or domestic use of surveillance software. Purpose of attack: Surveillance Software: Purchased off the shelf
	SOUTH AFRICA
53	South African Defense Review in 2014 said the country “requires the protection of its cyber-domain, through…a comprehensive information warfare capability.” Unit of Revenue Service used off-the-shelf Purpose of attack: Surveillance Suspected offensive teams: Military or intelligence Targets: Domestic Software: Developed in country, purchased off the shelf
	SOUTH KOREA
54	Announced in 2014 it would develop offensive cybercapabilities to respond and make pre-emptive strikes against North Korea. National Intelligence Service purchased off-the-shelf hacking software, which officials say Purpose of attack: Surveillance Suspected offensive teams: Military or intelligence Targets: Domestic, international Software: Developed in country, purchased off the shelf
	SPAIN
55	Allegedly behind sophisticated hacking tool called Careto, Spanish for “ugly face.” Clues indicatedesigners used Spanish language. Targets include Morocco and Gibraltar. But a former senior U.S. official said country’s Purpose of attack: Surveillance Suspected offensive teams: Military or intelligence Targets: International Software: Developed in country, purchased off the shelf
	SUDAN
56	Hacking software purchased by National Intelligence and Security Services, which have both domestic and Purpose of attack: Surveillance Software: Purchased off the shelf
	SWITZERLAND
57	Armed forces creating unit for “computer network operations,” or various types of offensive cyberwork, according to U.N. in 2013. Unclear level of sophistication. Purchased off-the-shelf surveillance Purpose of attack: Surveillance Suspected offensive teams: Military or intelligence Software: Developed in country, purchased off the shelf
	SYRIA
58	Pro-regime hackers—whose status in military is unclear—use “remote access trojans” to spy on opposition, by making adjustments to easily found criminal software. Syrian Electronic Army group conducts defacement Suspected acts: 2011-present: Espionage against opposition forces. 2013: Associated Press Twitter account hacked by Syrian Electronic Army to falsely claim White House had 2014: Hundreds of media sites hacked by the Syrian Electronic Army through online commenting system. Purpose of attack: Surveillance, defacement Suspected offensive teams: Private groups Targets: Domestic, international

Software: Developed in country

THAILAND

59 Purchased off-the-shelf surveillance software; law enforcement denies domestic use.

Purpose of attack: Surveillance

Suspected offensive teams: Military or intelligence

Targets: International

Software: Purchased off the shelf

TURKEY

60 Cyber Warfare Command created. National Police purchased off-the-shelf hacking gear.

Purpose of attack: Surveillance

Suspected offensive teams: Military or intelligence

Targets: Domestic, international

Software: Purchased off the shelf

TURKMENISTAN

61 Off-the-shelf hacking software found running on server with IP address assigned to government ministry of

Purpose of attack: Surveillance

Software: Purchased off the shelf

UNITED ARAB EMIRATES

62 Off-the-shelf software detected targeting human-rights activist. Early surveillance software found on

Purpose of attack: Surveillance

Targets: Domestic

Software: Purchased off the shelf

U.K.

63 Works with the U.S. on certain cybertools, according to experts and documents revealed by former NSA

Suspected acts:

2012: British spies with GCHQ, the signals intelligence branch, hack Belgacom to spy on phone customers in

Malware includes: Regin, used in Belgacom attack, also linked to Australia and others.

Purpose of attack: Surveillance

Suspected offensive teams: Military or intelligence

Targets: Domestic, international

Software: Developed in country

UKRAINE

64 Suspected acts:

2014: Hackers claiming to support government hack Russian targets, including officials' emails.

Purpose of attack: Surveillance, defacement

Suspected offensive teams: Private groups

Targets: International

UZBEKISTAN

65 Purchased off-the-shelf surveillance software.

Purpose of attack: Surveillance

Software: Purchased off the shelf

VIETNAM

66 Rights groups say malware used for domestic surveillance. Military has spoken of developing a cyberprogram

Suspected acts:

2010: Google and McAfee say malware used to spy and enact denial-of-service attacks on potentially tens of thousands of Vietnamese users. McAfee says perpetrators have some allegiance to government.

2013: Vietnam-based Associated Press reporter, American activist and others receive emails meant to trick

Purpose of attack: Surveillance, defacement

Suspected offensive teams: Private groups
Targets: Domestic, international
Software: Developed in country, purchased off the shelf

Policy/short description
67 Suspected acts:
Purpose of attack:
Suspected offensive teams:
Targets:

Policy/short description
Suspected acts:
Purpose of attack:
Suspected offensive teams:
Targets:

Policy/short description
Suspected acts:
Purpose of attack:
Suspected offensive teams:
Targets:

Policy/short description
Suspected acts:
Purpose of attack:
Suspected offensive teams:
Targets:

Policy/short description
Suspected acts:
Purpose of attack:
Suspected offensive teams:
Targets: