Vetting the Global Supply Chain
A New Approach to Reducing Risks of Information and Communication Technology Product Acquisition
# Table of Contents

- Executive Summary ......................................................... 2
- Why Vetting the ICT Supply Chain Is Vital .......................... 3
- Risks in the ICT Supply Chain ........................................... 4
- Three Strategies for Due Diligence 2.0. ............................... 6
- A New Approach for Evaluating ICT Supply Chain Risks ......... 9
- Delivering a Comprehensive Solution ................................. 11
Federal agencies and commercial organizations are more dependent than ever on the global supply chain. In particular, the provision of information and communication technology (ICT) products and services relies on complex, ever-changing relationships between third-party suppliers, affiliates, joint ventures, and sub-contractors around the world. The supply chain affords cost and production efficiencies but also poses a variety of real risks that can threaten quality, national security, and economic stability. Buyers and prime contractors in the supply chain must conduct due diligence and thoroughly vet third-party suppliers to ensure that offerings are genuine, meet all specifications, and are not compromised by global threat actors or competitors. New laws and regulations for federal agencies and commercial contractors also require additional efforts in supply chain risk management.

Typical scrutiny of suppliers is a one-time event occurring prior to award of a contract. Due diligence often relies on information provided by the prime contractor via questionnaire. Unfortunately, this level of assessment barely scratches the surface of a complex supply chain. Booz Allen Hamilton, a leading strategy and technology consulting firm, recommends a new approach to systematically deepen visibility of risks and ensure the quality and safety of acquired products and services. The new approach leverages three themes:

- **Continuous monitoring** throughout the product life cycle
- **Use of many sources and types of data**—especially newly developed capabilities for acquiring and performing deep multidimensional analytics with open source “big data”
- **Expanded scope of vetting** to include sub-contractors in the ICT supply chain.

With the new approach to ICT supply chain risk management, federal agencies and commercial contractors can reduce risks and improve confidence in fulfilling their missions.

### Public Incident: Pre-infected Product

**CHALLENGE**

In Sept. 2012, Microsoft’s digital crime researchers bought 20 new PCs from factories in China; four were infected with viruses by criminals attempting to exploit insecure supply chains. The PCs were running counterfeit versions of Microsoft Windows with the Nitol virus, which reported back to a command and control center hosted by 3322.org – a site hosting 500 different strains of malware.

**SOLUTION**

Microsoft received permission from a US court to take down the network of Nitol-infected computers.

**RESULTS**

Nitol enables criminals to create back doors into attached networks; other malware at 3322.org was capable of switching on a victim’s microphone or web camera and record keystrokes, allowing access to their log-on credentials and accounts.
The modern manufacture and provision of products and services rely more than ever on the global supply chain. It’s rare when a single provider controls the entire process for making and delivering all components of an offering—particularly for complex information and communication technology. More than half of products made are “intermediate” or semi-finished, intentionally built as a component of another product. The same is true for services, where more than 70 percent are intermediate in nature.

For organizations consuming ICT products and services, the global supply chain provides many benefits such as efficient logistics, speed of acquisition, lower cost, higher availability, and effective inventory control. According to research by Booz Allen, the highest priority for buyers is security and integrity of end use products, and the potential for compromise is a serious risk—not just for government and commercial buyers, but also for sellers who use components and sub-systems from third-party providers within the supply chain. Risks may affect providers of either ICT hardware or software products.

The US Department of Defense (DoD) defines supply chain risk as follows: 

[The risk that an adversary may sabotage, maliciously introduce unwanted function, or otherwise subvert the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of a covered system so as to surveil, deny, disrupt, or otherwise degrade the function, use, or operation of such system.]

Ultimately, responsibility for vetting the supply chain rests with organizations consuming its products and services. Understanding the various risks associated with the ICT supply chain is the first step to successfully vetting suppliers and the security and integrity of their offerings.

---

3. “Covered systems” are defined by the DoD as any IT or telecommunications system used for intelligence, national security, military command and control, weapon or weapons system, or critical to fulfillment of military or intelligence missions.

“With the new approach to ICT supply chain risk management, federal agencies and commercial contractors can reduce risks and improve confidence in fulfilling their missions.”
Risks in the ICT supply chain originate from complex characteristics that inherently favor attackers. A supply chain has many “moving parts” that are difficult to see and evaluate. Their dispersed global nature means distance, cultural, and language barriers can shroud potential risks that may originate with mistakes due to sloppy processes and controls, deliberate criminal intent, or influence by enemy nations, rogue organizations, or terrorists. Tracing links between numerous suppliers and sub-suppliers in the chain is challenging—particularly if any of them wish to keep buyers unaware of third-party outsourcing—and lack of transparency abounds.

As a result, buyers may experience a wide range of potential risks. Examples of supply chain risks include counterfeit parts, espionage using compromised devices, reverse engineering, intellectual property (IP) theft, and cyber threats. Supply chain risks may affect buyers and prime contractors in different ways, as listed in the sidebar.

Risks in the ICT supply chain may also trigger penalties to primary contractors for non-compliance with laws and regulations on procurement risk management. These can include loss of right to sell to federal agencies, loss of reputation and trust, and other fallout such as loss of revenue and market capitalization. New laws and regulations are described in the sidebar on page 8.

### Risks in the ICT Supply Chain

#### Risks and Fallout in the ICT Supply Chain

<table>
<thead>
<tr>
<th>Risks</th>
<th>Fallout for Federal Buyers</th>
<th>Fallout for Prime Contractors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Counterfeit parts</td>
<td>Product will not perform to specification, malware propagation, potential interruption of national services, compromise of national security, injury or loss of life</td>
<td>Product will not perform to specification, loss of contract and revenue</td>
</tr>
<tr>
<td>Espionage using compromised devices</td>
<td>Interruption of national services, compromise of national security, injury, or loss of life</td>
<td>Interruption of business operations, loss of contract and revenue</td>
</tr>
<tr>
<td>Reverse engineering</td>
<td>Exposure of classified IP to enemies, compromise of national systems and services</td>
<td>Loss of IP to competitors, loss of revenue</td>
</tr>
<tr>
<td>IP theft</td>
<td>Exposure of classified IP to enemies, compromise of national systems and services</td>
<td>Loss of IP to competitors, loss of contract and revenue, potential criminal charges for loss of classified IP</td>
</tr>
<tr>
<td>Cyber threats</td>
<td>Vital national services slow down or stop functioning due to denial of service, advanced persistent threats and other cyber threats from terrorists, nation states, or hacktivists</td>
<td>Vital business services slow down or stop functioning, loss of contract and revenue</td>
</tr>
</tbody>
</table>

### Public Incident: Counterfeit Software

**Challenge**
An investigation by Immigration and Customs Enforcement discovered the chief scientist of a US government contractor obtained pirated software from Chinese and Russian cyber criminals via Crack99.com. The industrial-grade software was used in performing contracts for military and law enforcement.

**Solution**
Perpetrators were sentenced to prison.

**Results**
The scientist used the pirated software (several were on the restricted export list) to conduct computer simulations on components being designed for use in the Black Hawk helicopter, the Presidential helicopter fleet, Patriot missile components, and law enforcement technology.
The risks mentioned are especially pertinent to providers of ICT products and services using commercial-off-the-shelf (COTS) components, which are required by the federal government whenever possible. The risks are less likely to trusted manufacturers providing high assurance products to DoD, such as nuclear submarines or weapons systems.

To illustrate one area of risk in more depth, consider the iconic issue of supply chain risk: counterfeit parts. The risk of buying counterfeit parts is particularly important as they form the unseen bedrock of technology-based solutions for national security and defense. Over the last decade, the growth in global reports of counterfeit parts has been surging (see Figure 1). Government agencies and commercial buyers alike are trying to execute their missions “faster, better, cheaper” and as a result, are more likely to fall prey to unscrupulous sellers offering discounted parts.

When counterfeit parts do not conform to required standards, their use in operational systems may degrade or trigger undesirable functionality. In the US, several operational systems have had significant operational delays due to the use of counterfeit parts—including military satellites and GPS systems.

Sub-standard counterfeit parts also contribute to shorter time-to-failure and reduced lifespans of components and sub-systems (see Figure 2).

As noted in the sidebar, there are many other supply chain risks in addition to counterfeit parts. It is crucial for federal buyers of ICT to thoroughly vet the supply chain and minimize risks for ICT used in critical functions affecting national security. This includes acquisition program engineering offices, sustainment organizations, and acquisition agencies such as the General Services Administration, Defense Logistics Agency, and Defense Information Systems Agency.

Figure 1. ERAI Suspect Counterfeit or High-risk Part Incidents

Figure 2. Typical Electronic Parts Failure Characteristics


Three Strategies for Due Diligence 2.0

Three strategies can help buyers improve the vetting process. These strategies include continuous monitoring; using many sources and types of data for vetting; and expanding the scope of vetting to include sub-contractors in the ICT supply chain.

**CONTINUOUS MONITORING.**

Typical vetting occurs just once: prior to awarding the primary contract. This one-time practice puts buyers at risk of exploitation because the complex global supply chain is constantly changing over the multiyear life cycles of ICT solutions. What mattered early in the procurement process may be irrelevant later, and new risks that appear later will be undetected if vetting occurs just once. To effectively assess and manage risks in the ICT supply chain, buyers need to move from one-time checks to continuously monitoring potential vulnerabilities throughout the product or service life cycle. Continuous monitoring of the supply chain is also important for security professionals whose mission is to protect ICT solutions deployed within their organizations—especially due to the universal exposure to cyber threats.

Continuous monitoring should seek insight into the ability of a supplier to perform on a contract, and watch vendors for key events triggering risk, such as new cyber threats, geo-political events, change of ownership, new locations, changes to key personnel, different customers, different ownership structure based on mergers and acquisitions, and new contracts with potential enemies or competitors.

---

**Global4Sight Case Study**

**Assessing supply chain vulnerabilities to make informed decisions on risk**

**CHALLENGE**

A government client required assistance in understanding the risk of companies performing research and development on new, emerging technologies. The field of possible manufacturers developing these new technologies varied from small, sole proprietorships to large, multinational corporations with multiple global business partners. The client was concerned about the following risks:

+ Quality/counterfeit products that could put safety of personnel and operations at risk
+ Threats from personnel inside the company disclosing sensitive technology information
+ Business relationships with companies in countries with poor intellectual property records
+ Cyber threats from embedded malware or Trojans capable of stealing proprietary information

The client did not have a method for assessing risk to prioritize the use of their resources on only the most relevant companies.

**SOLUTION**

Global4Sight™ Supply Chain Risk Assessment analysts employed open source research and analysis against a proprietary risk framework, developed through years of supply chain assessments with both government and commercial clients, to evaluate the commercial vulnerability of the new technologies across seven distinct attributes. Booz Allen’s supply chain vulnerability framework is a proven, repeatable process that we tailor to specific client needs. Using the framework, our Global4Sight team conducted a quantitative and qualitative risk assessment of more than 500 companies across 11 different technologies.

**RESULTS**

Upon completing the risk assessment, Booz Allen delivered a prioritized list of companies that presented the highest risk, and helped incorporate them into the client’s threat analysis process to be considered for additional research and/or operational activities. By removing the client’s burden of conducting research and analysis on the hundreds of companies developing new technologies, the client was able to reallocate time, money and resources on performing more mission critical tasks.
Continuous monitoring needs ongoing attention, so it's important to establish adequate support for this process that should extend throughout the life cycle of a product or service.

**USE MANY SOURCES AND TYPES OF DATA.**

Expanding the sources and types of data used for vetting is another strategic priority. The typical process of vetting an ICT product or service provider consists of looking at data self-reported by a prime contractor via questionnaire. This approach has several issues: the information is single source; it may not be objective; and the scope of information is narrow and often one-dimensional. Using multiple sources and types of data will help improve the odds of a thorough vetting.

**Supplier/Vendor Provided Data.** This is the traditional source of information for vetting risks. It usually includes product specifications; sourcing information for sub-components; and background information on the company, key employees, security processes, and so forth.

**Buyer-collected Data.** This type of data is particularly valuable when a federal agency or prime contractor has been buying finished products or sub-components from a vendor for many years. The category does not apply to a new contractor.

**Closed Source Data.** These are received by request from a supplier or sub-contractor. Private source data may include tax documents, internal reports, reports privately commissioned to third parties, interviews with company executives and technology experts, and so forth.

**Open Source Data.** These are publicly available—sometimes for free, sometimes for a cost from third-party service providers. The nature of open source data (or “big

---

**Public Incident: Cyber Attack**

**CHALLENGE**

RSA makes widely used security tokens, which were compromised in March 2011 by phishing emails containing a zero-day exploit that allowed attackers to access the corporate network and install anything they wanted.

**SOLUTION**

RSA patched the zero-day exploit and its customer who discovered the breach (Lockheed Martin) had its telecomuters work at company offices for a week. RSA also issued new RSA SecurID tokens and had the passwords reset for all 133,000 employees.

**RESULTS**

A major online attack was launched against Lockheed Martin in May 2011, attempting to exploit its VPN access using compromised RSA SecurID token seeds. The attacks were detected immediately by Lockheed and no data was compromised.
data”) examined depends on requirements specified by your particular evaluation framework (see Section IV). Using open source data will help cast a wider net of analysis over your extended supply chain. The diversity of open source data allows you to create a rich, composite picture of risks. It comes from broadcast media, social media, company websites, company marketing literature, public financial filings and investor communications, business publications, newspapers, social media, government websites, data aggregator services, and other sources such as the Government and Industry Data Exchange Program (GIDEP).

In the past, using open source data was not an option because there was, and continues to be so much of it. New technologies and automated processes have lifted this restriction, and now allow evaluators to gather, integrate, analyze, and present the information in practical and meaningful ways. By using open source data, procurement evaluators can dramatically expand the scope of vetting the ICT supply chain risk to a degree that has never before been possible—and extract actionable insights that reduce the risks of using ICT products and services.

**EXPAND VETTING SCOPE.**

Typically, vetting is limited to the prime contractor and not the entire related ICT supply chain. An objective vetting process needs to go deeper than this by assessing all entities involved with producing parts, components, sub-systems, and services for the final solution. This is a new requirement specified by emerging laws and regulations on ICT procurement (see sidebar).

Section IV introduces a new approach to systematically implement these strategies for comprehensive risk assessment of the ICT supply chain.

<table>
<thead>
<tr>
<th>LAWS AND REGULATIONS ON SUPPLY CHAIN RISKS IN ICT PROCUREMENT</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Comprehensive National Cybersecurity Initiative (CNCI)</strong></td>
</tr>
<tr>
<td><strong>Defense Federal Acquisition Regulations Supplement (DFARS) Interim Rule 2012-D050</strong></td>
</tr>
<tr>
<td><strong>Intelligence Community Directive 731</strong></td>
</tr>
<tr>
<td><strong>“Wolf Provision”</strong></td>
</tr>
</tbody>
</table>
A New Approach for Evaluating ICT Supply Chain Risks

Booz Allen recommends a comprehensive new approach to systematically strengthen ICT supply chain assessment. The new approach uses a flexible framework to help buyers incorporate strategies to improve supplier vetting described in Section III. Our supply chain vulnerability framework is a proven, repeatable process that we tailor to specific client needs. It strengthens assessments by seeking risk data in a holistic manner, which requires the perspective of multiple dimensions. The dimensions or risk attributes that apply to your agency or business may vary. Often your organization will require consideration of unique dimensions of risk. Examples of some of the dimensions may include:

**Location** – Vulnerabilities associated with firm location based on US friendly and business environment.

**Ownership** – Vulnerabilities associated with identities and affiliations of firm owners.

**Business Relationships** – Vulnerabilities based on foreign affiliation of the partner and the strength of the relationship (e.g., customer, vendor, strategic partner, joint venture).

**Key Personnel** – Vulnerabilities associated with biographic information of key personnel (e.g., C-suite, program managers, key technical staff).

**Reputation** – Vulnerabilities associated with the standing of the firm and key persons.

**Security** – Measures taken to protect information, products, and operations from insider and/or physical breaches.

**Financial Stability** – Vulnerabilities associated with the financial stability of a firm over time including merger and acquisition activities, and financial issues.

**Geo-Political** – Vulnerabilities caused by tensions specific to a particular country or region of interest.

**Cybersecurity** – Cyber threats directed against supplier network, product, or services such as distributed denial of service (DDoS), loss of personally identifiable information, etc.

Each dimension of risk, such as those noted above, in turn requires evaluation and monitoring for a unique range of differently weighted sub-risks. For example, in the dimension of Business Relationship, monitoring for foreign influence could include the following elements that gradually increase vulnerability to supply chain risk:

+ Principally US partners with weak relationship types (least vulnerable)
+ US partners with some foreign activity and strong relations
+ Partners from friendly countries with strong relationships or non-friendly/competitor with weak relations
+ Partners from non-friendly/competitor countries with strong relationships
+ Partners with strong links to foreign governments and strong relationships (most vulnerable)

The complexity of analyzing multidimensional data such as these means a solution should allow buyers to rank data attributes into a scorecard format to quickly synthesize meaning for actionable insights.

**THIRD-PARTY ASSESSMENTS.** Buyers can gain significant benefits by using a third-party assessor for vetting the ICT supply chain. Benefits include independent objectivity; expert knowledge and experience in assessing risk; dedicated resources for continuous risk assessments throughout the product or service life cycle; comprehensive assessment of potential risks in a prime contractor’s ICT supply chain; technology and sources for comprehensive data collection; and data analytics and reporting for insightful, actionable insights.
Delivering a Comprehensive Solution

Comprehensive, continuous, and objective evaluation of risks in the ICT supply chain is critical for buyers in federal agencies and commercial companies. To help organizations effectively vet their ICT supply chains, Booz Allen’s Predictive Intelligence services offer Global4Sight Supply Chain Risk Assessment.

This service combines a strong heritage of cloud architecture and applications development with leading-edge open source and social media research and intelligence analysis tradecraft to provide actionable information on global threats and global market opportunities. Our Global4Sight analysts employ open source research and analysis against a proprietary risk framework, developed through years of supply chain assessments with both government and commercial clients, to evaluate the commercial vulnerability of the new technology across distinct multidimensional attributes. Our supply chain vulnerability framework is a proven, repeatable process that we tailor to specific client needs.

We invite your organization to tap the benefits of our new approach to ICT supply chain risk management, reduce associated risks, and improve confidence in fulfilling your mission.

See our ideas in action at boozallen.com
About Booz Allen
Booz Allen Hamilton has been at the forefront of strategy and technology consulting for more than 100 years. Today, Booz Allen is a leading provider of management consulting, technology, and engineering services to the US government in defense, intelligence, and civil markets, and to major corporations and not-for-profit organizations. In the commercial sector, the firm serves US clients primarily in financial services, healthcare, and energy markets, and international clients primarily in the Middle East.

Booz Allen helps clients achieve success today and address future needs by applying functional expertise spanning consulting, analytics, mission operations, technology, systems development, cybersecurity, engineering, and innovation to design, develop, and implement solutions. The firm’s management consulting heritage is the basis for its unique collaborative culture and operating model, enabling Booz Allen to anticipate needs and opportunities, rapidly deploy talent and resources, and deliver enduring results. Booz Allen helps shape thinking and prepare for future developments in areas of national importance, including cybersecurity, homeland security, healthcare, and information technology.

Booz Allen is headquartered in McLean, Virginia, employs more than 22,000 people, and had revenue of $5.48 billion for the 12 months ended March 31, 2014. Over the past decade, Booz Allen’s high standing as a business and an employer has been recognized by dozens of organizations and publications, including Fortune, Working Mother, Forbes, and G.I. Jobs. More information is available at www.boozallen.com. (NYSE: BAH)