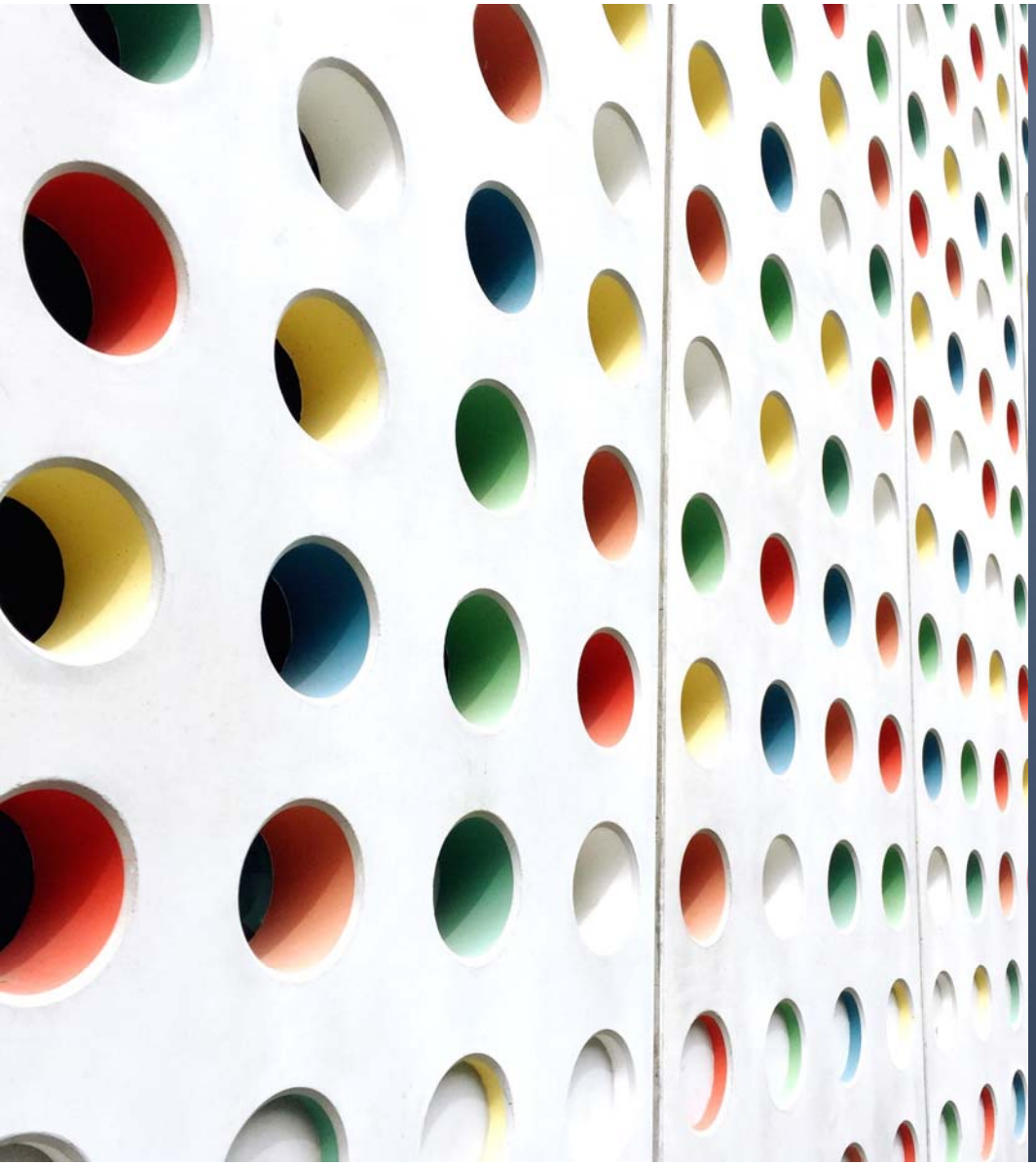

Supply Chain Security

Supplier/Contractor Relationships in Negotiated Contracts

December 14, 2022

for

ISSA-Central Maryland Chapter

Introduction

Todd Hinson

- MS Engineering, Cybersecurity Policy and Compliance (GWU)
- > 30 years experience in IT, Law, and Contracting
- Speaks Geek, Legalese, and Business
- Cybersecurity Contracts Principal with Constellation Energy (in Balmer hon!)
- All around great guy with a quirky sense of humor ☺

- I am not an attorney nor do I offer legal advice … my comments and opinions here today are my own and do not represent ISSA, my employer, past employers, or any governmental agency. Hypothetical breach or cybersecurity scenarios are presented for illustrative purposes and are not related to ISSA, my employer, past employers, or any governmental agency, or any insider knowledge of any specific organization. The presentation is for educational purposes only and should not replace independent professional judgement or research. Topics covered during the presentation are high-level and should be considered conceptual elements to a larger understanding of cybersecurity, negotiated contracts, and third-party or supply-chain management.

Supply Chain Security

WHAT IS IT?

WHY SHOULD I CARE?

HOW IS IT DONE?

What Is It?

- The Supply-Chain has been stressed to its very limits and Vendor/Supplier and Third-Party relationships have been similarly stressed with the “trust but verify-verify-verify” protocol meaning more today, than ever before.
- Supply Chain Security:
  - materials and services delivered when needed and where needed
  - materials and services delivered with integrity, according to buyer specifications
  - Integrity & Availability elements of the CIA Triad for Information Security

Why Should I Care?

- Information Systems need supplies, both materials and services, but more precisely, secure Information Systems need secure supplies, from trusted providers who will deliver trustworthy materials or services which arrive according to exact order specifications, unadulterated.
- Goal in negotiated contracts is to not deal with HW, SW, or PW (peopleware) vulnerabilities in the first place and to have contract protections in place for when vulnerabilities become security events.
- Selecting trustworthy vendors; defining the relationship with a high degree of security-based granularity; and protecting the Firm via remedies and insurance provisions, will increase the overall Information Systems' Security, by building a solid foundation out of trustworthy blocks.

How Is It Done?

- Know Your Security Requirements
  - Policies and Procedures
  - Cybersecurity Frameworks
  - Regulatory Regimes
  - Industry Specific Guidelines
- Designate Your "Must Haves"
  - Notice and Reporting
  - Access Grant and Removal
  - Compliance
  - Insurance and Liability
- Communicate with Negotiators
  - Supply Professionals
  - Legal
  - Leadership
- Memorialize in Agreements
  - RFPs, RFQs, Bids, etc.
  - SOWs
  - Contracts
  - Purchase Orders/Change Orders
  - NDAs
  - MOUs (Memo of Understanding)
  - MAA (Mutual Assistance Agreement)

Know Your Security Requirements

- Description from the Business Stakeholder (intent view)
- Solution Vetted by IT Architects (actual view)
- Connectivity
- Access Controls
- Data in Use, in Transit, at Rest
- On-Site and Remote Access
- REMEMBER: You are working toward an Agreement where (Intent = Actual = Contract)

Cybersecurity Frameworks and Regulatory Regimes

- ISO/IEC 27001, COBIT
- NIST CSF
  - NIST 800-53
  - NIST 800-171
- FAR and DFARS
  - FAR 52.204-21, -23 thru -26
  - DFARS 252.204 thru 7008-252.204-7021
- FISMA and FedRAMP
- CSA Cloud Controls Matrix
- NERC
  - North American Electric Reliability Corp
  - Reliability Standards
  - CIP Standards
    - Critical Infrastructure Protection
- NRC
- U.S. States
  - CCPA
  - NYDFS
- E.O. (Executive Orders)
- GDPR

Designate Your “Must Haves”

- Notice and Reporting
- Access Grant and Removals
- Compliance
- Insurance and Liability

Communicate with Negotiators

- Supply Professionals
  - Frontlines and Under Appreciated
  - Stock Language with Minor Tweaks
- Legal
  - Nice but Not Too Nice
  - Custom Language
  - Geek-speak, Legal-speak, Business-speak
- Leadership
  - Bring in the Hammer
  - Game of Chicken / Train in the Tunnel
  - The Closer

Memorialize in Agreements

- RFPs, RFQ, Bids, etc.
- SOWs
- Contracts
  - General / Master Terms and Conditions
  - Exhibits
  - Attachments
- Purchase Orders and Change Orders
- NDAs
- MOUs (Memo of Understanding)
- MAA (Mutual Assistance Agreement)

Meeting of the Minds

- Defined Terms … how it might look
- "Cybersecurity Incident": A cybersecurity event that has been determined to have an impact on the organization prompting the need for response and recovery. [NIST Glossary of Terms]
- "Cyber Security Incident" means any malicious act or suspicious event, or group of suspicious events occurring during the performance of, or in connections with the Services to be provided under the Agreement, that is a Compromise, or has the potential to be a Compromise, of the Digital Materials or Digital Services provided by Acme Corporation.

Meeting of the Minds

- Defined Controls … how it might look
- "Access Enforcement | Role-based Access Control": Enforce a role-based access control policy over defined subjects and objects and control access based upon [Assignment: organization-defined roles and users authorized to assume such roles]. [NIST 800-53 Rev. 5, Control Catalog, AC-3(7)]
- Acme Corporation will use RBAC (Role-Based Access Control) to approve and authorize contractor personnel access to confidential information, protected systems, or other client data, exchanged during the performance of the Services. The RBAC implementation must conform with NIST 800-53 Rev. 5, AC-3(3) "Mandatory Access Control" for personnel with access to Personally Identifiable Information (PII).

Meeting of the Minds

- Defined Controls … how it might look
- "Least Functionality | Binary or Machine Executable Code": (a) Prohibit the use of binary or machine-executable code from sources with limited or no warranty or without the provision of source code; and (b) Allow exceptions only for compelling mission of operational requirements and with the approval of the authoring official. [NIST 800-53 Rev. 5, Control Catalog, CM-7(8)]
- Acme Corporation will not insert any code in any Application, Firmware, System Software, or Security Patch which is not authorized or which would have the effect of disabling functionality or otherwise shutting down all or a portion of any Digital Material supplied under the Agreement, or which would damage information stored within the Digital Materials supplied under the Agreement.

Trust but Verify, Verify, Verify

- Audits and Spot Checks
  - Internal and External
- Evidence Documents
  - SOC Reports
  - Certifications
  - Attestations
  - Policies and Procedures
  - DRP/BCP
  - Pen Tests and Vulnerability Scans
- See Something!, Say Something!

- What Did I miss?
- Questions?
- Examples?