

Compliance is a Culture: Leading Change from the Inside Out

Joe Sullivan

DIB Prime Contractor - Principal Cybersecurity Compliance Analyst
Lt Col (Ret) – Air Force Cyberspace Operations Officer
Ph.D. Candidate – Information Systems and Communication, Robert
Morris University, Pittsburgh, PA

Agenda

- Why Cybersecurity
- Myths
- DIB Challenges
- Change the Culture
- The Future

“...results show that organizational culture, awareness in cybersecurity, and employee involvement strongly predict information security compliance behavior. In addition, trust in senior management was also discovered to mediate the influence of organizational factors on compliance..”



Ghaleb, M. M. S., & Pardaev, J. (2025). Controlling cyber crime through information security compliance behavior: Role of cybersecurity awareness, organizational culture and trust in management. *International Journal of Cyber Criminology*, 19(1), 1-26. <https://doi.org/10.5281/zenodo.476619101>



Why CMMC, Frameworks, Special Publications,
ISO...?

If we are here, we all (most) agree upon the following:

- Cyberthreats are real
- Adversaries are looking to steal
 - Intellectual Property
 - Trade Secrets
 - Personal Data
 - Government Data
- Protection of data is absolutely required
- Compliance with government, industry standards, and corporate policies is required and needed.

If you don't agree, we can debate afterwards.

Why are we doing this cybersecurity thing?

- System/Software Security Flaws
- Hardware Flaws
- Policy Threats
 - Password complexity/length
 - Authentication
 - Complete access
- Social Engineering
- External attacks
- Insider Threats
- Users

...AND!!!! The U.S. Government Shares USASpending.gov

https://www.usaspending.gov/search?hash=6088a069cb327b6dde44949ced186338

tes | SSO | IBM | Employee | Bridge Sites | MBSE Assess Questi... | Regulations-Procur... | AI CORE - Home

Advanced Search Filter by: Prime Awards and Transactions

Filters

Learn which data elements are associated with certain search filters

Submit

Reset filters

Keyword

Search by Keyword

microprocessors

Time Period

Fiscal years Custom dates

FY 2025 FY 2024 FY 2023 FY 2022

FY 2021 FY 2020 FY 2019 FY 2018

FY 2017 FY 2016 FY 2015 FY 2014

FY 2013 FY 2012 FY 2011 FY 2010

FY 2009 FY 2008

Show New Awards Only

Award Type

Agency

1 Active Filter: Learn how active filters work

KEYWORD

microprocessors

Prime Award Results

Contracts 895 Contract IDVs 5 Grants 109 Direct Payments 0 Loans 0 Other 1


| Prime Award ID | Recipient Name | Obligations | Outlays | Award Desc |
|----------------|------------------------------------|----------------|---------|---|
| 0043 | DRS NETWORK & IMAGING SYSTEMS LLC | \$9,597,851.00 | -- | THE FOLLOV (SYSTEM BX |
| 0021 | ALLIANT TECHSYSTEMS OPERATIONS LLC | \$5,012,687.47 | -- | AN/AAR-47 M AND MICROI |
| GST1004EC0031 | I.T.S. CORPORATION | \$1,700,007.78 | -- | TASK DESCF PART OF TH |
| 0040 | OTTO BOCK HEALTHCARE LP | \$1,300,000.00 | -- | ADVANCED I |
| N6554006C0020 | YORK INTERNATIONAL CORPORATION | \$1,218,883.00 | -- | DUPLEX MIC |
| FA702223F0085 | TELEDYNE BROWN ENGINEERING, INC. | \$1,126,927.00 | -- | ATMOSPHEF MICROPROC SYSTE... read |
| W81XWH22C0049 | LIBERATING TECHNOLOGIES INC | \$1,099,358.84 | \$0.00 | AWARD OF L CONTRACT I |
| FA850907C0031 | DRS SUSTAINMENT SYSTEMS INC | \$1,035,333.00 | -- | ECP 52- DEV MICROPROC read more |


To quote an NCIS agent:


“Only 3% of the IP addresses hitting this site are based in the United States.”

<https://www.usaspending.gov/search>


AWARD PROFILE Contract Summary


 Agency Details >

 Parent Award Details >


 Place Of Performance ▾


| | |
|------------------------|--|
| Address | FORT IRWIN, CA 92310-5095 UNITED STATES |
| Congressional District | CA-23 ⓘ |

 Period Of Performance >


 Legislative Mandates >

| | |
|-----------------------------|---|
| Recipient | I.T.S. CORPORATION |
| Recipient Identifier | KNKZYDQKL3D1 (UEI ⓘ) |
| Parent Recipient | I.T.S. CORPORATION |
| Parent Recipient Identifier | KNKZYDQKL3D1 (UEI ⓘ) |
| Recipient Address | 300 E. ESPLANADE STE 1450 OXNARD, CA 93036-1238 UNITED STATES |
| Congressional District | CA-26 ⓘ |
| Business Types | Category Business Foreign Owned Not Designated a Small Business Special Designations |

 Acquisition Details

 Competition Details

⋮ Additional Details

 Executive Compensation

| | |
|-----------|------------------------------|
| Officer 1 | JOHN CURTIS [REDACTED] |
| Officer 2 | DEBORAH OLIVER [REDACTED] |
| Officer 3 | KENT MATLICK [REDACTED] |
| Officer 4 | VERNON BROADWATER [REDACTED] |
| Officer 5 | JOHN SUTTON [REDACTED] |

Myths

- Guarding against cyber threats is not worth our resources
- Checklists are great... True, but...
 - Needed for initial system setups
 - Incident Response
 - Audits/Assessments
 - Outdated the minute they are finished
- Frameworks/Checklists are all we need
 - “there are no frameworks that match all of the ideal properties for all cyber resilience framework for SMEs.”

J. F. Carías, M. R. S. Borges, L. Labaka, S. Arrizabalaga and J. Hernantes, "Systematic Approach to Cyber Resilience Operationalization in SMEs," in IEEE Access, vol. 8, pp. 174200-174221, 2020, doi: 10.1109/ACCESS.2020.302

“It (cybersecurity) is an effort in protecting national space from **internal and external** threats of hackers, criminals, rival aggressors and other vulnerabilities of an unauthorized obtrusive into national vital data or attack on critical infrastructure.”

Sule, B., Sambo, U., & Yusuf, M. (2023). Countering cybercrimes as the strategy of enhancing sustainable digital economy in Nigeria. *Journal of Financial Crime*, 30(6), 1557–1574.
<https://doi.org/10.1108/JFC-07-2022-0157>

Stevens, T. (2016), *Cybersecurity and the Politics of Time*, Cambridge University Press, New York, NY.



DIB Supplier Challenges

- Suppliers are trying to do the right thing to support our service members
- Small and Medium Enterprises (SMEs) are struggling
- Limited Budgets
- Personnel
 - Training
 - Once trained, skills are highly sought after by other entities.

DIB Challenges (SMEs)

- Multi-Factor Authentication (MFA)
- Security Information and Event Management (SIEM)
- Security Operations Center (SOC)
- Training
- Reporting
- Plan Generation
- Cost
- CMMC - Number of CMMC Third-Party Assessment Organization (C3PAO) – Get started early

DIB Challenges (SMEs)

- Underdeveloped
 - Incident response plans
 - Internal phone numbers
 - External phone numbers
 - Listing of contractually required reports
 - Third party resources
 - Disaster recover
- Get to know your local FBI, CISA, NCIS, OSI, etc. representatives –
Your...
 - First call should **NOT** start with - “I’m Joe Sullivan from ABC Corporation and we are locked out of our system.”
 - Should start with – “Hey Rich, we have been hit with ransomware, and I’m calling Jack and Lisa next.”

DIB Challenges (SMEs and Large Corporations)

- Outstanding security plans don't match the systems they are protecting
 - Facility Drawings
 - BIOS Settings
 - Passwords
- BIOS protection
- Password complexity (add password website)
- Patching
- Outdated software and hardware
- CUI awareness and requirements (e.g. export controls)

“Cyberthreats are agnostic and they may affect the enterprises as a whole. However, SMEs are prone to be more intensively affected by some specific cyberthreats and attacks, in comparison to larger enterprises.”

Antunes, M., Maximiano, M., Gomes, R., & Pinto, D. (2021). Information security and cybersecurity management: A case study with SMEs in Portugal. *Journal of Cybersecurity and Privacy*, 1(2), 219-238. <https://doi.org/10.3390/jcp1020012>



Change the Cybersecurity Culture

“A culture that instills cybersecurity as a collective value undergirded by open communication, ethical leadership, and unambiguous expectations fosters a context in which compliance becomes a normative practice.”

- Corporate Cybersecurity Support – The “T³4CEOS”
 - Trust
 - Open communication
 - Ethical Leadership
 - Clear Directives and Understanding
 - Time
 - Crosstalk/Knowledge Transfer
 - Professional Education (all types)
 - Leadership Involvement
 - Training

Ghaleb, M. M. S., & Pardaev, J. (2025). Controlling cyber crime through information security compliance behavior: Role of cybersecurity awareness, organizational culture and trust in management. *International Journal of Cyber Criminology*, 19(1), 1-26. <https://doi.org/10.5281/zenodo.476619101>

Change the Cybersecurity Culture

- Policies
- Budgets
 - Personnel Training
 - Lunches
 - Technology
- Training
 - Center for Development of Security Excellence (CDSE) - <https://www.cdse.edu/>
 - Federal Bureau of Investigation (FBI)
 - Naval Criminal Investigative Service (NCIS) and Air Force Office of Special Investigations (OSI)
 - Cybersecurity & Infrastructure Security Agency (CISA)
 - Industry Sector Training

Change the Cybersecurity Culture

- Test each other – make it fun and educational
 - Validation of cybersecurity awareness
 - Major cyber actors targeting business
 - Competitors

“...employee engagement substantially moderates the link between cybersecurity awareness and information security compliance behavior.”

- Engage with your employees (tabletop exercises, trainings)
 - Educates employees on the process
 - Drives home the threat against the company
 - Reaction and awareness to threats (phishing, malware, ransomware)
 - Can be fun
 - Working lunches

Ghaleb, M. M. S., & Pardaey, J. (2025). Controlling cyber crime through information security compliance behavior: Role of cybersecurity awareness, organizational culture and trust in management. *International Journal of Cyber Criminology*, 19(1), 1-26. <https://doi.org/10.5281/zenodo.476619101>

Change the Cybersecurity Culture

- Gauge employee behavior towards cybersecurity and change it
 - Testing – Small incentives with a win
 - Questioning behavior – i.e. QUESTION EVERYTHING
 - Ensure they understand the threat is real

When “cybersecurity is viewed not only as an engineering imperative but as a shared organizational imperative, employees will be more inclined to embrace and adhere to security guidelines, even in discretionary circumstances where they are not being directly supervised.”

Ghaleb, M. M. S., & Pardaev, J. (2025). Controlling cyber crime through information security compliance behavior: Role of cybersecurity awareness, organizational culture and trust in management. *International Journal of Cyber Criminology*, 19(1), 1-26. <https://doi.org/10.5281/zenodo.476619101>

What is out there?

- Frameworks
- National Institute of Standards and Technology (NIST) Special Publications (SP)
 - NIST SP 800-53, Security and Privacy Controls for Information Systems and Organizations
 - NIST SP 800-171, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations
 - NIST SP 800-171A, Assessing Security Requirements for Controlled Unclassified Information
- Government Agency specific requirements
- Resources
 - CISA
 - FBI
 - Agency Specific
- Cyber AB

Future Thoughts (please provide your ideas)

- Shared cloud services
- Minimum technical standards to secure the network
 - Policies are needed/required but when?
 - Administrative vs. Technical controls
 - STIGS
- Tax relief for compliance/certification
- Cybersecurity grants
- Document only suppliers vs. Suppliers with electronic storage

Resources

(No need to recreate a plan, framework, training)

- DoD CIO Library - <https://dodcio.defense.gov/Library/>
- CISA Resources - <https://www.cisa.gov/resources-tools/all-resources-tools>
 - CSET: <https://www.cisa.gov/resources-tools/services/cyber-security-evaluation-tool-cset>
 - CISA Best Practices: <https://www.cisa.gov/topics/cybersecurity-best-practices>
 - CISA Tabletop Exercise Packages: <https://www.cisa.gov/resources-tools/services/cisa-tabletop-exercise-packages>

Resources

- C3PAO Shopping Guide for Small & Medium-Sized Businesses - <https://ndisac.org/defense-news/nd-isac-releases-c3pao-shopping-guide-for-small-medium-sized-businesses/>
- National Security Agency (NSA) Cybersecurity Services - <https://www.nsa.gov/About/Cybersecurity-Collaboration-Center/DIB-Cybersecurity-Services/>
- Federal Bureau of Investigations (FBI) - <https://www.ic3.gov/Outreach/PrivateSectorEngagement>
 - [InfraGard](#)
 - [Citizens Academy](#)

Resources

- Cyber AB - <https://cyberab.org/>
- CMMC Marketplace - <https://cyberab.org/Catalog#!/c/s/Results/Format/list/Page/1/Size/9/Sort/NameAscending>
- National Defense Information Sharing and Analysis Center (ND-ISAC) - <https://ndisac.org/>

Parting Thoughts

- Adversaries already in the network?!
- Not if, but when.
- Once they are in, what can they get?
- Invest in backups
- Know who to call!
- Know who you are CONTRACTUALLY obligated to call!!!!
- Continue to grow your cybersecurity knowledge and presence.
- Just Start!

“Cybersecurity is contemporarily a major determinate of national security, economic strength and digital opportunities.”



Sule, B., Sambo, U., & Yusuf, M. (2023). Countering cybercrimes as the strategy of enhancing sustainable digital economy in Nigeria. *Journal of Financial Crime*, 30(6), 1557–1574. <https://doi.org/10.1108/JFC-07-2022-0157>

Dunn Cavelt, M., & Wenger, A. (2019). Cyber security meets security politics: Complex technology, fragmented politics, and networked science. *Contemporary Security Policy*, 41(1), 5–32. <https://doi.org/10.1080/13523260.2019.1678855>



Questions?

Thank
you

Joseph Sullivan

412-609-7682

sullivanjo@rmu.edu