Cyber Awareness and Resiliency (CAR) Security and Privacy Controls for Information Systems and Organizations, NIST SP 800-53

Dr. Merrick S. Watchorn, DMIST, CEL, CPCI, CECI, CCIP, CII, CTFI, SMIA, MCIT, CCSK, SS

April 18, 2018

Background

- The United States has suffered numerous security breaches, incidents and an erosion of public trust within the last five years

- Reported Security Incident(s):
  - 2017 (376 - 154,055,666 affected)
  - 2016 (810 - 11,032,013 affected)
  - 2015 (535 - 160,018,638 affected)
  - 2014 (872 - 68,971,415 affected)
  - 2013 (886 - 60,940,933 affected)

  - 2013 – 2017 Security Incident(s): 3,479 – Affected: 455,018,665

- Department of Homeland Security (DHS) – US CERT CVE Attack Threat Vectors(s): 6,117

National Institute of Standards & Technology

- Tasked with building and dissemination of Commercial and, as of January 2014, Department of Defense (DoD) Cybersecurity Standards effective as of January 2016.

- NIST rate of Publication Metric(s):
  - 2013 (12) – including NIST SP 800-53r4
  - 2014 (15)
  - 2015 (37)
  - 2016 (44)
  - 2017 YTD (12) – including NIST SP 800-53r5

- The NIST SP 800-53r5 now aligns budget, training and accountability to OMB A-130, which created FedRAMP, FISMA, HIPAA, HITRUST, Cyber Security Framework and EO 13636.

Major Cyber Milestones (2016-2017)

- 2016 – Cyber Attacks increase by 35% from March – November 2017 including potential Russian concentric attack profiles.
  - July 2016
    - US Intelligence Led Cyber Attack Analysis started
    - FBI Investigation started
    - Joint Task Force, Led by NIST to build stronger Cyber Resilience started –US CYBERCOM starts nomination process to become a COCOM
  - August 2016
    - Dr. Ron Ross defines Cyberspace - “the security we currently have in place isn’t working, the reason: “You cannot protect that which you do not understand … Increased complexity translates to increased attack surface.
  - May 2017
    - EO - STRENGTHENING THE CYBERSECURITY OF FEDERAL NETWORKS AND CRITICAL INFRASTRUCTURE, signed
    - OMB M-17-05, M-17-25 both updated and released.
  - August 2017
    - NIST draft version of the SP 800-53, SP 800-181, SP 800-125A
      - removes 127 security controls
      - increases from 864 to 912
      - OMB A-130 guidelines are mapped to specific security controls and federal laws for accountability and liability standards are established.
      - Virtual Machines security standards and baselines security functions
      - CyberSecurity Workforce Framework

Impact Assessment

- The United States Government has gone to great lengths to overhaul its entire approach to Cybersecurity with a significant inference on training.
  - NIST SP 800-53r5 goes active 29 December 2017
    - Removes: Confidentiality, Integrity and Availability lexicon and replaced with Privacy and Assurance.
    - New Terms and Definitions are established to bring about higher security standards and breadth to its reach to include Internet of Things (IoT).
      - Required Controls: 52, OMB Controls: 92, Cyber Security Framework Controls: 234, Privacy Controls: 158, Assurance Controls: 344
      - Potential Federal Security Baseline Increase: 575 controls required as a starting point for all Federal Agencies.
      - Legal Impacts for Federal Contractors
      - Standardization of Confidential Unclassified Information terms
      - Keyword Search Index mapped to Controls
      - Policy Alignment (OMB, FISMA, FIPS, HIPAA, Privacy, ISO, etc.)
      - Training the means and method of determination of Cyber Resilience
  - Validation of Proof of Findings:
    - DoD asking for Cyber Certifications for everyone on an contract.
    - RFI's and RFP's have language to provide the USG the ability to scan networks assessing compliance. But will also be looking for security incidents. The language is clear, they intend to assess compliance, blue team, penetration test, etc. on networks.
    - US CERT authorized to conduct Cyber Investigations on behalf of OMB
    - US CERT turns over findings to the FBI
    - FBI has authorization from OMB to act on the findings of US CERT
    - Government Contractors standards for prosecution are now found within IRS, FBI, OMB, DHS and IC (CUI)

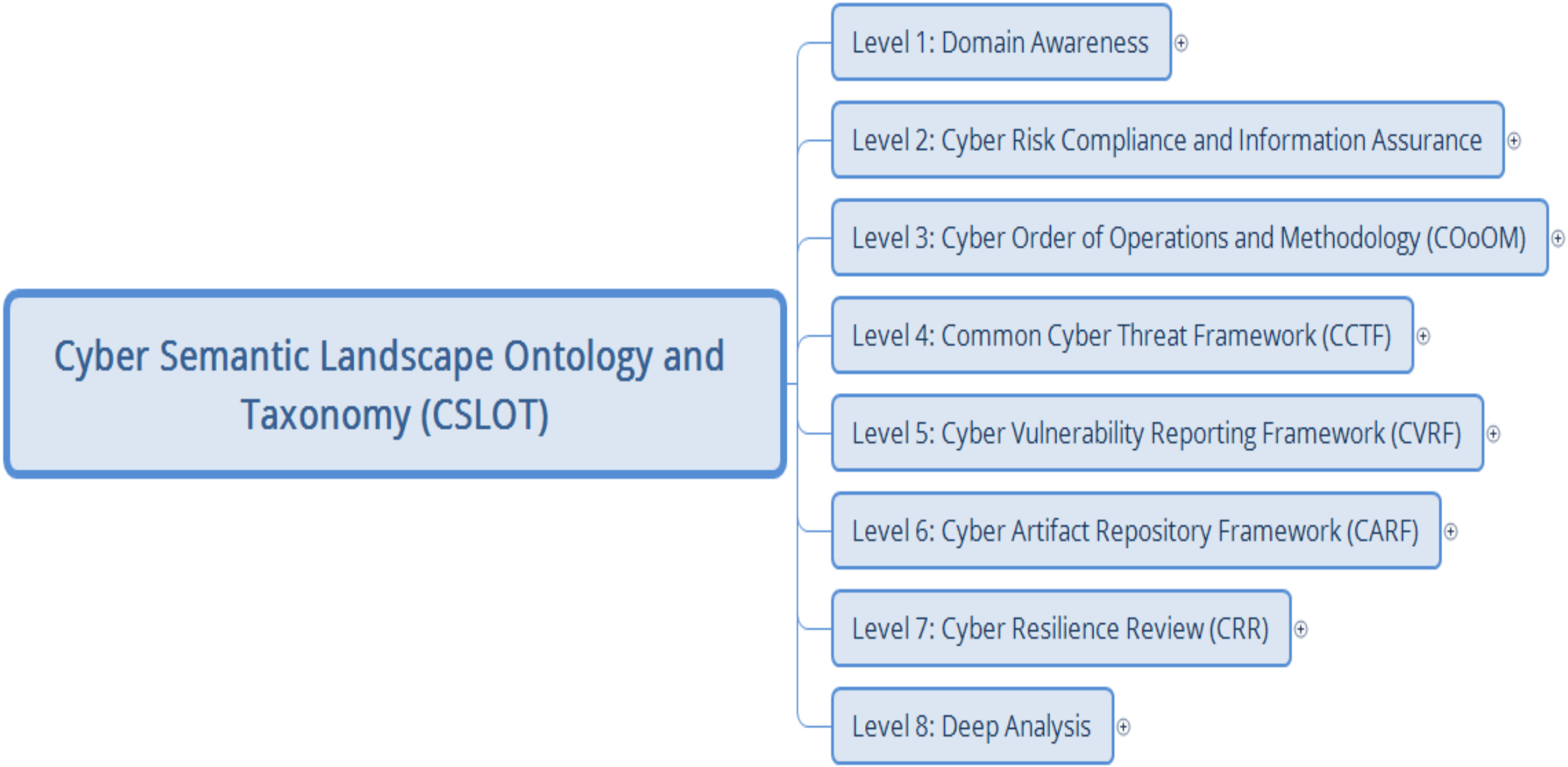
OMB Circular A-130 Requirements - Budget

RESPONSIBILITY	DESCRIPTION	OMB A-130	CONTROLS
General Requirements			
Establish and maintain a comprehensive privacy program	Agencies shall establish and maintain a comprehensive privacy program that ensures compliance with applicable privacy requirements, develops and evaluates privacy policy, and manages privacy risks	Main Body § 5(f)(1)(a); Appendix I §§ 3(b), 3(f), 4(e).	PA-1, PM-18
Ensure compliance with privacy requirements and manage privacy risks	Agencies shall ensure compliance with all applicable statutory, regulatory, and policy requirements and use privacy impact assessments and other tools to manage privacy risks. Agencies shall cost-effectively manage privacy risks and reduce such risks to an acceptable level	Main Body §§ 4(g), 5(e)(1)(d), 5(f)(1)(a); Appendix I § 3(a), 3(b)(4), 3(f), 3(g).	CA-1, IP-4, PA-1, PM-3, PM-9, PM-19

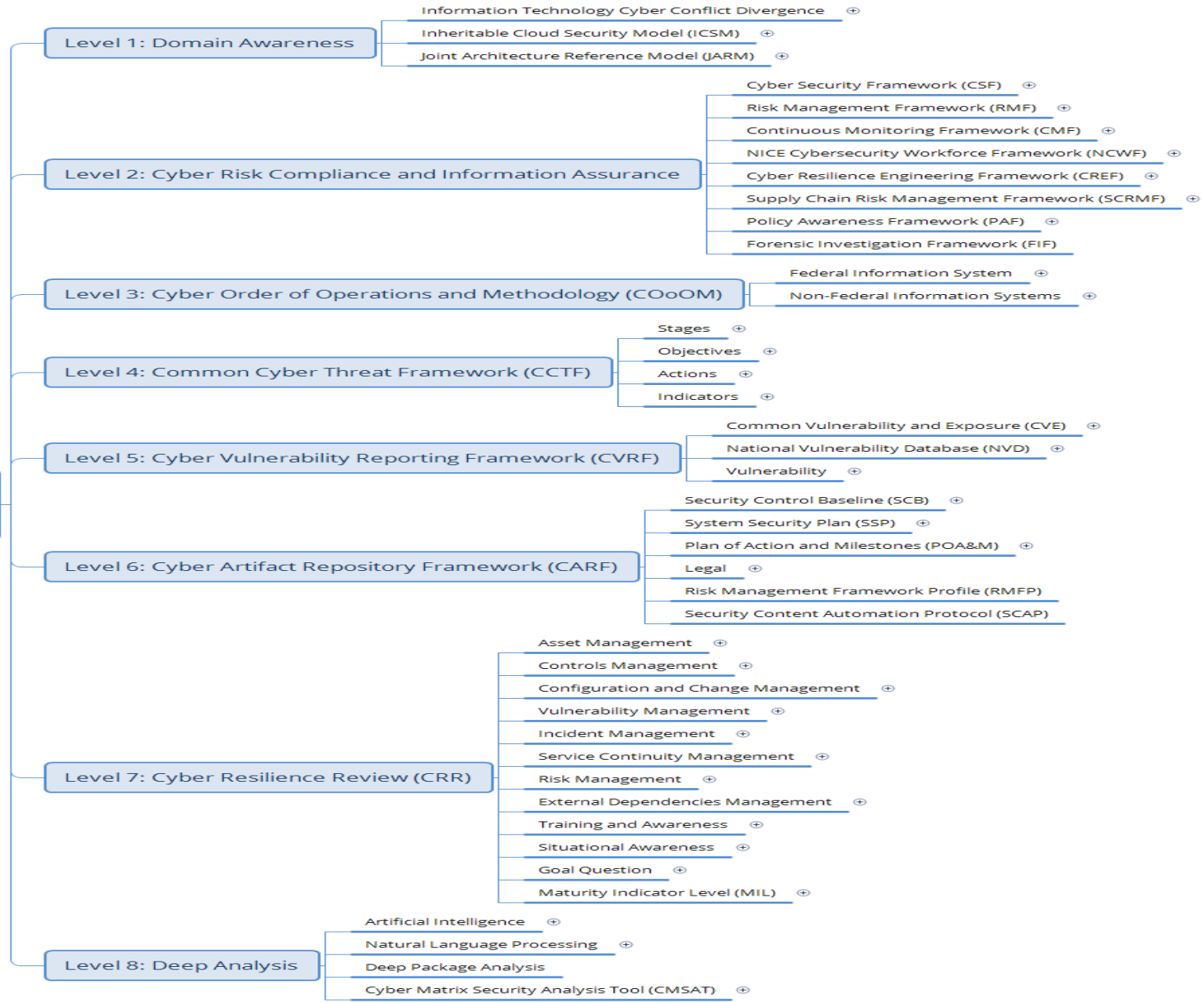
Example of Impact – USG Agency Statement

- Inspectable Security Practices – Roles performed by the Office of Security

- Leadership commitment to and involvement in the security program
- Security Training, Awareness & Education
- Threat identification, management and mitigation
- Physical Security Processes and Procedures
- Export compliance for classified contracts
- Program protection practices and procedures
- Counterintelligence program
- Insider Threat program
- DD254 and compliance
- Visitor control practices and procedures
- International Security and Foreign Nationals
- Incident response and reporting
- Control of classified materials
- Operations Security
- Configuration, management, auditing and protection of classified IT systems
- Emergency response practices and procedures
- Communications Security practices and procedures
- Classification management and Derivative classification
- Adverse reporting and security violation investigation and reporting
- Personnel Security Processes and Procedures



Cyber Semantic Landscape Ontology and Taxonomy (CSLOT)



Summary

- The ability to build and retain Cyber qualified expertise will continue to rise in cost.
- Individuals with critical skills sets will become in high demand and manpower attrition will rise.
- Training budget will have to dramatically increase to facilitate the development of a DoD level training command.
  - What does that mean for the industry workforce in cost?
  - Timing?
  - Will there be a transition time to become compliant?
- Poor decision-making processes associated with Cyber will have potential legal and contract award impacts.
- Ability to see Cyber scope increase with cost adjustments will become the norm.
- All federal contractors will have this problem and the first early adopters may win the lion share of the market.
- Without the Cyber Workforce Framework implementation and standard within an organization will cause over-time an erosion of contract awards and profitability.
- Business Development and Proposal ecosystem will have to become educated, understand the impacts, properly document and address Cybersecurity to the equivalent of Technical, Cost and Past Performance excellence in order to achieve USG awards.

Reference(s)

- Office of Management and Budget (OMB)
  - OMB A-130, FISMA, FedRAMP
- National Institute of Standards and Technology (NIST)
  - NICE Cybersecurity Workforce Framework (NCWF), NIST SP 800-181
  - Security and Privacy Controls for Information Systems and Organizations, NIST SP 800-53r5
  - Security Recommendations for Hypervisor Deployment, NIST SP 800-125A
- Department of Homeland Security (DHS)
  - US CERT Cyber Resilience, Cyber Attack Framework, Cyber Technique Framework
- Department of Justice
  - Federal Bureau of Investigations
    - Criminal Justice Investigation Service (CJIS)
- Committee of National Security System (CNSS)
- Congressional Research Service
  - Federal Laws relating to Cybersecurity: Overview of Major Issues, Current Laws, and Proposed Legislation