High Performance Computing (HPC) Security Control Baseline Revealed

In my role as a former CISO, I was always engaged at some level in the company in discussions about risk. What I quickly discovered is that these conversations roamed through many topics, many organizations (to include our customers), many levels of understanding and awareness, and, of course, many technologies and solutions. But through all this complexity, there was a common theme. Everyone didn't understand and only asked, "Please just tell me what to do so I can do my job." This lack of awareness and how it applies to each employee, and most importantly, to the organization, is why Cybersecurity is so hard and we are NOT defending against attackers well. Because of this "just tell me what to do" mentality that is pervasive as Cybersecurity has matured, we, security practitioners, have pavlovianly trained the world (including ourselves) into a "checklist" mentality.

I was talking with some IT professionals recently about the impact of the changing laws and requirements being levied in the Federal IT space. While one could argue that these common sense and comprehensive requirements for Information Security can apply to any organization (Federally funded or not), I will only address it from a Federal perspective to this discussion.

I was explaining in my discussion about how the very technologies and architectures we are leveraging to help us are inherently insecure. The supply chain is accepted without vetting. Virtual Technologies, Hypervisors and Cloud implementations we trust inherently yet they hold the keys to the kingdom and nobody truly assesses them. The concept of resiliency and recovery are becoming dominant discussions in Cybersecurity over traditional defense and protection because we are not successful in defending postures.

Through the realization that Cybersecurity is highly complex and evolving, personnel are not Cyber Aware and technical solutions are not vetted, assessed and resilient. NIST is trying to address these Cyber security challenges through its series of Special Publications. I co-authored a document called Cybersecurity Awareness and Resiliency (CAR). This document attempts to outline the philosophy one must adopt to ensure understanding and governance in a Cybersecurity program of any organization.

However, I posited that most organizations ignore these NIST guidelines justified by their Risk Management program decisions. This violates the CAR tenants. Too often, I hear statements like, "I'll accept that risk", or an organization puts "weighting" on Cyber risk so that they can rationalize lower funding or accelerate product/service delivery without really

High Performance Computing (HPC) Security Control Baseline Revealed

addressing the Cyber risk. That rationalization manifests itself in many other ways. But how can a discussion without Cybersecurity technical jargon simply explain the responsibilities an organization finds themselves? The common way is a comprehensive technical survey (the tool of choice by insurance brokers, auditors, etc.). I think most people will agree, this is a low-impact, time consuming and low-value endeavor. What if we can simplify?

So, I began by asking some questions:

1) Does your organization accept Federal funding in some form or fashion?
2) Does your organization transmit, store or process Privacy information of any kind?
3) Does your organization transmit, store or process Privacy information from the EU?
4) Does your organization require Common Criteria?
5) Does your organization require solutions be "behind" the DHS TIC?
6) Does your organization worry about Insider threats?
7) Does your organization worry about Advanced Persistent Threats?

Based on these answers, one can begin to see a picture of requirements form. Each of these questions creates an angle in the Cybersecurity Order of Operations Methodology (COoOM). An angle is a singular reference that means there are security control considerations unique to it that must be accounted for and scored in our COoOM score for unbiased and scientific measurement of possible security control scoring against known security control requirements.

Now, the question in my conversation that I was discussing was about how does all the NIST guidance affect and change how we approach technology implementation? The technology in question was Virtualization. But that conversation quickly devolved into a larger superset – High Performance Computing (HPC). So, the question we kept bouncing around, how does the NIST expect Cyber security to be applied to a Federal HPC system? The first thing we should do is understand that we need to increase our Awareness – per the CAR. That means we must research (be aware) of all applicable guidance.

Our first question was, do you accept funding from the Federal government? If yes, then the US Office of Management and Budget, through OMB Circular A-130 has deemed everyone must follow these security controls in our first angle score.

High Performance Computing (HPC) Security Control Baseline Revealed

If you are under OMB oversight, then Cybersecurity Framework (CSF) applies. That introduces new mandated controls in our next angle.

If you transmit, store or process PII, we now have many more controls that are required in our next angle.

If your PII collection includes EU citizens, then GDPR applies. That introduces a new angle and its controls.

If Common Criteria is required, then a new angle of controls needs to be identified. This is encapsulated in ISO 15408 and its associated controls:

If your solution requires the US Department of Homeland Security (DHS) Trusted Internet Connection (TIC), then this introduces new controls and a new angle in the COoOM.

If Insider Threat is mandated or you are worried about it, then you now have these controls and a new angle.

If you are worried about Advanced Persistent Threat, then you need to ensure you have these controls in your new angle.

Our next research for CAR is to see where NIST guidelines provides insight into our solution. We see that there are MANY guidelines that apply. For instance:

NIST SP 500-299 (Draft) – NIST Cloud Computing Security Reference Architecture

NIST SP 800-18rev1 – Guide for Developing Security Plans for Federal Information Systems

NIST SP 800-23 – Guidelines to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products

NIST SP 800-25 – Federal Agency Use of Public Key Technology for Digital Signatures and Authentication

High Performance Computing (HPC) Security Control Baseline Revealed

NIST SP 800-29 – A Comparison of the Security Requirements for Cryptographic Modules in FIPS 140-1 and FIPS 140-2

NIST SP 800-30rev1 – Guide for Conducting Risk Assessments

NIST SP 800-32 – Introduction to Public Key Technology and the Federal PKI Infrastructure

NIST SP 800-34rev1 – Contingency Planning Guide for Federal Information Systems

NIST SP 800-35 – Guide to Information Technology Security Services

NIST SP 800-36 – Guide to Selecting Information Technology Security Products

NIST SP 800-37rev1 – Guide for Applying the Risk Management Framework to Federal Information Systems: a Security Life Cycle Approach

NIST SP 800-37rev2 (Draft) – Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy

NIST SP 800-39 – Managing Information Security Risk: Organization, Mission, and Information System View

NIST SP 800-40rev3 – Guide to Enterprise Patch Management Technologies

NIST SP 800-41rev1 – Guidelines on Firewalls and Firewall Policy

NIST SP 800-44rev2 – Guidelines on Securing Public Web Servers

NIST SP 800-46rev2 – Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security

NIST SP 800-50 – Building an Information Technology Security Awareness and Training Program

NIST SP 800-51rev1 – Guide to Using Vulnerability Naming Schemes

NIST SP 800-53Arev4 – Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans

High Performance Computing (HPC) Security Control Baseline Revealed

NIST SP 800-53rev4 – Security and Privacy Controls for Federal Information Systems and Organizations

NIST SP 800-53rev5 (Draft) – Security and Privacy Controls for Federal Information Systems and Organizations

NIST SP 800-55rev1 – Performance Measurement Guide for Information Security

NIST SP 800-59 – Guideline for Identifying an information System as a National Security System

NIST SP 800-60 VOL 1rev1 – Guide for Mapping Types of Information and Information Systems to Security Categories

NIST SP 800-60 VOL 2rev1 – Guide for Mapping Types of Information and Information Systems to Security Categories: Appendices

NIST SP 800-61rev2 – Computer Security Incident Handling Guide

NIST SP 800-63x series [Digital Identity Guideline series]

NIST SP 800-64rev2 – Security Considerations in the System Development Life Cycle

NIST SP 800-86 – Guide to Integrating Forensic Techniques into Incident Response

NIST SP 800-88rev1 – Guidelines for Media Sanitization

NIST SP 800-92 – Guide to Security Log Management

NIST SP 800-115 – Technical Guide to Information Security Testing and Assessment

NIST SP 800-122 – Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)

NIST SP 800-123 – Guide to General Server Security

NIST SP 800-125 – Guide to Security for Full Virtualization Technologies

NIST SP 800-125A – Security Recommendations for Hypervisor Deployment on Servers

High Performance Computing (HPC) Security Control Baseline Revealed

NIST SP 800-125Arev1 (Draft) – Security Recommendations for Server-based Hypervisor Platforms

NIST SP 800-125B – Secure Virtual Network Configuration for Virtual Machine (VM) Protection

NIST SP 800-126rev3– The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.3

NIST SP 800-126A – SCAP 1.3 Component Specification Version Updates: An Annex to NIST Special Publication 800-126 Revision 3

NIST SP 800-137 – Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations

NIST SP 800-144 – Guidelines on Security and Privacy in Public Cloud Computing

NIST SP 800-147 – BIOS Protection Guidelines

NIST SP 800-147B – BIOS Protection Guidelines for Servers

NIST SP 800-150 – Guide to Cyber Threat Information Sharing

NIST SP 800-155 (Draft) – BIOS Integrity Measurement Guidelines

NIST SP 800-160 VOL1 – Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems

NIST SP 800-160 VOL2 – Systems Security Engineering: Cyber Resiliency Considerations for the Engineering of Trustworthy Secure Systems

NIST SP 800-161 – Supply Chain Risk Management Practices for Federal Information Systems and Organizations

NIST SP 800-171rev1 – Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

NIST SP 800-171A – Assessing Security Requirements for Controlled Unclassified Information (Final Draft)

High Performance Computing (HPC) Security Control Baseline Revealed

NIST SP 800-175A – Guideline for Using Cryptographic Standards in the Federal Government: Directives, Mandates and Policies

NIST SP 800-175B – Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms

NIST SP 800-181 – National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework

NIST SP 800-184 – Guide for Cybersecurity Event Recovery

NIST SP 800-190 – Application Container Security Guide

NIST SP 800-192 – Verification and Test Methods for Access Control Policies/Models

NIST SP 800-193 – Platform Firmware Resiliency Guidelines

NIST SP 1800-11 (Draft) – Data Integrity: Recovering from Ransomware and Other Destructive Events

Now, if you read through this list, I know your first reaction is WOW. That is too much to consume and manage and this is just the Special Publications. However, please note that I did NOT list NIST guidance that is vendor, product or architecturally specific. Once decisions about the solutions are made, then this list grows based on these decisions. This list applies to all systems that aspire to conform to NIST guidelines (that is mandatory for Federal systems and any system funded by Federal funds). There are even US Government Request for Proposals (RFP) that specially call out, you MUST abide by ALL NIST guidance INCLUDING DRAFT publications. So, how do you bring this into an approach to address everything and NOT miss anything? This is where the application of the Cybersecurity Semantic Landscape Ontology and Taxonomy (CSLOT) comes into play. (Please feel free to read this separately.)

In today's compliance-oriented Cybersecurity World and/or Risk based organizations, we focus on compliance and checklists. What is the minimally required? Therefore, we get hacked. We are NOT addressing Cybersecurity for good hygiene and resiliency comprehensively in our designs. We are not addressing true security. We focus on passing audits. Even worse, these audits are based on "best practices", "audit organizations' checklists", or worse, vendor's security checklists or attestations and not real security.

High Performance Computing (HPC) Security Control Baseline Revealed

I have read through some articles on LinkedIn recently where there is a debate about how to score Cyber security risk. I was disappointed to read that many people believe that risk scoring should be weighted by the organization's desires. Or the organization should draft their own risk factors to successfully score. Really? When I was in school, I would LOVE to have the ability to create my own scoring criteria for my work!! Nothing but straight A's 😊. This is the poor state that the US has found itself in Cybersecurity, trying to define itself into simplicity by doing minimally relevant security. All grading and auditing, by definition, is against a standard. So, what is the standard? I outlined the many defined standards that are required by authorities for us to achieve in the questions above. We now must implement these security controls and have them properly assessed. How do we assess the proper implementation of a security control? That is an entirely different topic. But suffice it to say, it requires an evidentiary based assessment of every state of each security control to get "credit" for the successful implementation. Then, per DHS, we need to implement continuous monitoring of the assessments of security controls to show that the desired Cybersecurity posture does not change, again, all at an evidentiary level.

So, to come back to my CISO discussions, how can we score to help people understand true Cybersecurity without bias? How can this be based on scientific and mathematical models rather than an arbitrary "best practice"? Therefore, we created the COoOM. It is a litmus test to explain the likelihood of success against each angle and comprehensively.

If we answer yes to the above 7 questions, here is the basic COoOM model:

OMB A-130 – Federally funded systems require these controls: 65

FIPS 199 – Federally funded systems require these controls: 17

FIPS 200 – Federally funded systems require these controls: 1

NIST CSF – Federally funded systems require these controls: 257

Privacy – Adds Privacy controls from NIST SP 800-53: 36

CUI – Privacy adds CUI controls from NIST SP 800-171: 122

Assurance – Assurance adds these controls: 315

High Performance Computing (HPC) Security Control Baseline Revealed

EU PII – Requires GDPR adds these controls: 186

Common Criteria – requires ISO 27001 & 15408 and adds these controls: 186

ITM – Required controls for ITM adds: 87

APT – Required controls for APT adds: 64

DOJ FBI – Required controls for CJIS DOJ and FBI oversight and adds: 308

Resiliency Requirements adds: 193

Supply Chain adds: 19

Suddenly, again, we feel overwhelmed…

How can we apply this to a solution or approach? This is where Eigenspace did the research and can now provide security control baselines for many different possible modalities. In our conversation above, we were concerned with a Federal HPC solution. So, we want a High-Performance Computing Security Control baseline based on scientific research on the requirements and not best guesses, best practices, arbitrary checklists or auditor's focus areas.

Assimilating this guidance, Eigenspace is prepared to state that the NIST HPC baseline has 727 starting controls to select from and begin the justification process for the control removal process. This is NOT to say that the baseline is the only controls required for a solution. Keep in mind, every solution is required to have a System Security Plan (SSP). And, in this SSP, you must articulate the system's purpose, its system type, the type of data, the architectural choices, security boundaries, the dissemination platform (on Prem, cloud, hybrid, etc.), the technology and vendor choices, etc. These all will continue to drive more security control decisions. BUT, this HPC baseline is the minimum starting point for HPC implementations to be compliant with requirements for a Federal HPC system. The COoOM score also provides us a scoring mechanism to show the Cybersecurity posture of the proposed solution against known Security Controls by angle of focus.

To determine a given security control's importance to your approach it should be calculated using the COoOM Scoring system. One of the controls found within the suggested baselines is AT-2 – Awareness Training, which meets the following conditions:

High Performance Computing (HPC) Security Control Baseline Revealed

OMB:	Yes
FIPS 199:	No
FIPS 200:	No
CSF 1.1:	Yes
Cyber Resiliency:	No
Privacy:	No
Assurance:	Yes
Insider Threat Model:	No
Advance Persistent Threat:	No
DoJ FBI:	Yes
GDPR:	Yes
ISO 27001:	Yes
ISO 15408:	No

The formula for this calculation is made by our simple COoOM Importance Score: { 6 / 13 } = 46.153%. For each control in your baseline, simply count the angles and divide by the maximum angles of your COoOM to derive your own internal ranking systems for the controls. Eigenspace has taken this scoring model and extrapolated a comprehensive model for all angles called the *EigenScore*. If you would like to understand how your solution can be scientifically scored following this approach, please visit www.eigenspace.us for more explanation and contact information.

For Additional Information Contact:

Eigenspace
312 Main Street, Suite 300
Gaithersburg, MD 20878
240-654-4097
www.eigenspace.us