PUBLIC SUBMISSION

As of: 3/14/22 6:21 PM
Received: March 13, 2022
Status: Pending_Post
Tracking No. l0p-dv3y-46z0
Comments Due: April 25, 2022
Submission Type: Web

Docket: NIST-2022-0001
Evaluating and Improving NIST Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management

Comment On: NIST-2022-0001-0001
RFI-2022-03642

Document: NIST-2022-0001-DRAFT-0005
Comment on FR Doc # N/A

Submitter Information

Name: Jennifer Rose
Address:
Hampton Bays, NY, 11946

General Comment

See attachment for additional detail and citations.

SUMMARY

Automate NIST CSF for the critical infrastructure public and private sector. With different agency/industry versions with control standards instead of guidance. It will be instructive and structured with drop downs, yes/no statements and check boxes instead of text-based answers. Text based answers will only be required for explanation as to why any user may choose to disregard a control standard. These answers could help form updates to the tool.

Incorporate the NICE Framework into the system and setup will include identifying the requisite staff and have them complete their portion of the CSF, RMF and NIST 800 control series aligned to their NICE role and perform an electronic attestation.

Receive concurrence from all of the Federal and State Regulators covering each agency to agree to standardize their Cyber and Privacy regulations on the NIST CSF and 800 series. Their standards incorporated into the sector specific NIST 800 series will involve their input. Then regulatory Cyber and Privacy examinations will only be by exception of any serious issues identified by the tool. There will be workflow incorporated with thresholds, notification to internal NICE Framework leadership and also the ability to identify and sign off on the corrective actions required by the tool.

There will be different sections of the tool, one of which will be Supply Chain. Once a subject identifies their vendors, the vendors will then go through the same NICE Framework, CSF, RMF and NIST 800

control series disclosure and electronically sign off.

This tool will not address the various breach notification laws. But NIST's Frameworks and control sets will exponentially reduce the likelihood of breaches. And if DHS has access to portions of this data, they may be able to interrupt attacks in-flight and/or implement defensive measures to protect vulnerable sensitive data.

This tool may negate the need of State Data Privacy laws because it could incorporate existing Federal laws that are presently not enforced into the control standards.

Attachments

Attachment 1_Jennifer Rose Response NIST RFI-2022-03642

RFI Response

Requesting Party	NIST
RFI Deadline	April 25, 2022
Docket Number	22021-0045
Federal Register Doc	2022-03642
Document Citation	87 FR 9579
Page	9579-9581

Responding Party	Jennifer Rose
Date of Response	March 11, 2022
Email	
Phone	
Company	
Affiliation	None

RFI Title	"Evaluating and Improving NIST Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management"
Instructions	This RFI focuses on Evaluating and Improving the NIST Cybersecurity Framework (CSF) and Evaluating and Improving Cybersecurity Risk Management
Respondent Qualifications	Twenty-five years' experience in Governance, Risk and Compliance (GRC) roles within the critical infrastructure private sector, primarily in Financial Services. This also includes regulated program management roles in Tech, Utilities and Telecom. My early career focused on loss prevention before I transitioned into software development, then regulated project management and ultimately data governance and security program management. My technological expertise involves engineering, operations, training, service management, data center infrastructure, data governance, data science, cloud, storage and archive, service delivery, business continuity, contracts and vendor management.
Respondent Conflicts	None
Disclaimer	Any thoughts expressed or legal interpretation are my own. Nothing contained within should be construed as legal advice. This RFI response is solely focused on the NIST CSF and the 800 control series in the critical infrastructure public and private sector, and the vendors that support these critical sectors. I refrain from making any legislative suggestions. Although I recognize there is a fine line between regulatory guidance and law. Correctly inferring guidance is necessary to achieve compliance. I am very fortunate to have been employed by institutions and enterprise that take cybersecurity very seriously. I learned a lot from those experiences. Whenever I mention entities that struggle with cyber compliance, I am referring to those I interviewed with or short engagements excluded from my resume. I also recognize that NIST is a non-regulatory agency to promote U.S. innovation and industrial competitiveness by enhancing standards and technology in ways that enhance economic security. The tech sector's fundamental truth is that unless you identify root cause, you cannot fix a problem. The Federal Government is presently very focused on cybersecurity, which is resulting in a lot of new laws and pressure on NIST to come up with new guidance. This is making it harder for institutions, because it does not address root cause. I am focused on the root causes within

	this RFI response. While some of my recommendations may fall outside NIST's mission, perhaps some of the solutions I am recommending could provide insight to other agencies and also the critical infrastructure private sector leadership. I intentionally exclude the DoD from this proposal because they have their own programs that cover technological certification (CMMC), CUI training and a software system that assesses risk (eMASS) in the Defense Industrial Base.
Response Structure	Proposal 1. Executive Summary 2. Attributes of the proposed solution to enhance adoption of the NIST Cybersecurity Framework 3. Business case in support of the proposed NIST CSF solution 4. Attributes of the proposed solution to enhance NIST Supply Chain Risk Management 5. Business case in support of the proposed NIST Supply Chain Risk Management solution 6. Proposed solution caveats, comments and exceptions 7. Citations
SECTION 1 Executive Summary	I want to start off by expressing my gratitude to NIST for providing structure and maturation to cybersecurity governance. Your exhaustive guidance is fundamental to our economic and national security. In 2022 our lives depend upon automation. Our technological evolution also dictates brevity and intelligence. While the Government still relies primarily on documentation, the private sector depends upon digital tools. My recommendation to increase NIST CSF adoption is to turn NIST guidance into an application with sector specific decision support and automated risk scoring. The GDPR (General Data Protection Regulation) is the harmonization of data protection and privacy regulations throughout Europe. The European Union recognized that the complexity and volume of competing regulations had a deleterious effect on cybersecurity. We find ourselves in an even worse situation in the United States. I say this as someone who has made a career in support of data protection laws. I applaud the various agency efforts to add new cybersecurity laws and guidance in this swiftly moving threat landscape. We have brilliant data protection laws, we now need a uniform and automated way to implement them. The NIST 800 series began in 1990 to support the security and privacy needs of information systems for FISMA (Federal Information Security Management Act). There is a lot of confusion in the critical infrastructure private sector concerning FISMA, who it applies to and how to comply with it. The critical infrastructure public and private sector is unable to enforce FISMA compliance on their vendors, yet that is expected of them. Another common perception is that there are conflicts between Federal and State data protection regulations and that agency guidance and examinations are not based upon the NIST 800 series. Many private sector entities have separate teams managing each information protection regulation as an individual compliance program. But spending so much time and money on manual documentation-based compliance is defeating any potential benefit of these laws. Just as government agencies compete for budget, the same situation exists in the private sector. The Supreme Court, commercial insurers and numerous legislative bodies have cited the NIST CSF and 800 series as the acceptable technological standard of care. NIST 800-101 was cited 3 times in the Supreme Court's June

	24, 2014 Riley v California ruling[1]. The NIST CSF is also often mentioned in State regulations relating to data protection and privacy. At this point in our cyber maturity we need more than guidelines, especially when Regulators often assess or fine an entity for not achieving a guideline. We are able to define acceptable control standards. This is what I suggest that NIST undertake, clarifying and automating data protection and privacy standards on the NIST 800 series. **In order to increase adoption, compliance with NIST CSF needs to be achievable. If you leave security up to someone's best judgement, it will fail.** **The application solution I am proposing will also endeavor to harmonize the Federal and State data protection and privacy regulations, thereby increasing the likelihood of the private sector being able to institute meaningful and defensible cyber programs, in addition to cutting costs associated with manual duplicative compliance efforts.**

SECTION 2
 	
Attributes of the Proposed Solution to Enhance Adoption of the NIST Cybersecurity Framework
	The NIST Cybersecurity automation solution I propose is a decision support and risk scoring tool:
	
	1. It can potentially be built using existing no-code commercial software
	2. I envision this tool will frequently require control updates to reflect legislative and threat changes
	3. It should not be modifiable or configurable by users
	4. It would not involve uploading documentation nor divulging information that the Government is not already entitled to know
	5. There should be different versions for each industry sector
	6. Within each sector, there could be different levels just as there is with NIST 800-53
	   a. In accordance with FIPS 199[2], the system could make the decision about which level is appropriate depending upon factors such as whether or not the entity produces or processes Controlled Unclassified Information (CUI), their contracts and customer base
	7. It could be used by any entity that needs to comport to FISMA, including government agencies, regulated institutions or the critical infrastructure private sector
	   a. It can guide those using the tool about why and how they need to comport to FISMA
	8. It could provide detailed control guidance, decisions and accountability
	   a. If the user decides not to follow any control requirement in the tool, in accordance with Sarbanes-Oxley (SOX)[3] and the OMB 12/6/21 FISMA directive[4] the person who made that decision can justify why and electronically sign-off
	   b. SOX is required of all public companies and any entity required to comport to FISMA:
	      i. FAR Part 9[5] and 16[6]
	      ii. DFARS Part 232[7]
	      iii. The 2020 Holding Foreign Companies Accountable Act[8] identifies the three foreign nations that do not comport to SOX[9], but it also requires disclosure to the SEC about foreign government involvement in private companies
	   c. The detailed guidance for each control can be the result of consultation with DHS and Regulators:
	      i. As an example, sector specific laws may require log or record retention schedules that exceed anything commonly known to a Certified Public Accountant (CPA)
	      ii. This detail may not be included in vendor contracts but is very difficult for vendors to manage, especially those who serve numerous sectors and are required to schedule the retention and automated expiration of logs and records
	      iii. A tool such as this may eventually incorporate record and log retention guidance, decisions and attestation

	9. Please recognize that the largest institutions in the world struggle with interpreting how to implement NIST 800-53 controls just as much as SMB, maybe even more so due to the complexity of cyber and privacy laws they have to comport to 10. As a result of this regulatory discovery undertaken to automate control standards, likely additional categories of CUI will be identified and need to be added to the Controlled Unclassified Information National Archives[10] 11. The tool can also help users identify their CUI, the types they have, where it is, how it is protected and who has privileged access to it 12. Taking into account the NICE Framework[11], each section could be completed by the corresponding Manager responsible for the control family or function a. When each entity is setting up their account, they can identify their employees corresponding to the NICE Framework and then those employees could receive notification to complete their section as well as provide additional identifying information if they have privileged access or knowledge of their vulnerabilities b. The NICE Framework would likely need some modification for applicability to the private sector, mostly pertaining to job titles, the COSO Enterprise Framework[12] and clarifying certain regulatory staffing requirements c. SOX requires securing the data integrity pertaining to decisions, authorization and reporting audit trail 13. This system could be built utilizing structured data, so that risk metrics can be derived and reported to senior leadership within the organization completing the survey a. These metrics can then be reported to DHS to conform with the OMB requirement for agency automated risk reporting[4] b. According to the Oxford English Dictionary a technological metric is defined as "a system or standard of measurement" which presumes that a metric is not subjective and it cannot be derived from documentation or text 14. Any anomalies detected can automatically be reported to internal leadership and given a severity score a. This will address SOX internal and Board of Director risk reporting requirements[13] 15. Depending upon the severity threshold, Regulators may be notified to conduct additional inspection or provide guidance 16. A project such as this is perhaps best implemented in phases, one which could be a Federal and State regulatory crosswalk feature for each NIST 800-53 control a. Then Regulators could conduct examinations by exception and dedicate staff to develop expertise to specific NIST 800-53 control families
SECTION 3 Business Case in Support of the Proposed Solution to Enhance Adoption of the NIST Cybersecurity Framework	1. I view the NIST CSF as the Cybersecurity Governance hierarchal project plan's critical path 2. Once automated it can instruct users as to the prerequisite workstreams a. My experience is that many employees in regulated institutions and government vendors believe that the NIST 800 series is optional and so too is FISMA b. This system could also serve as an annual FISMA compliance audit[14] 3. The solution can provide customized control guidance throughout the process a. For instance, an Acceptable Use Policy in a regulated critical infrastructure institution that handles CUI requires specific baseline attributes[15] b. Government vendors that solely function as contract vehicles can require their subcontractors to complete both sections of the tool, this flow-down function can also be automated 4. The system could be built solely using structured data such as drop downs, check boxes and yes/no statements, so that reporting and metrics can be easily derived 5. This tool could be used as a knowledge base to guide NIST as to what the knowledge gaps are

6. It could be structured so it requests information from the user, but if the user answers a question inappropriately, the tool could then provide guidance on how to bring that function or control into compliance
    a. Once it provides corrective guidance, depending upon the criticality, worfklow enabled by the initial NICE Framework setup notifies the user's leadership that there is a control or function requiring conformance
    b. In accordance with SOX audit requirements, it will not let users change answers without leadership attesting to the corrective change having been implemented
7. The system can also have embedded workflow for non-conformance follow up with pre-configured time frames and escalation workflow depending upon the criticality
8. Zero Trust[16] does not just apply to access control, it pertains to who has vulnerability insight
    a. Critical infrastructure vulnerability data is CUI[17]
    b. This system incentivizes compliance through accountability because automated internal escalations and external oversight only becomes engaged through non-conformance
9. The world is struggling from a shortage of cybersecurity staff, so often GRC is staffed by those who have no or little technical background, nor any regulatory experience.
    a. This happens in Government as well as the private sector
    b. This provides no benefit to the regulatory examination or the institution's risk posture
    c. In my experience, regulatory examination escalations are often the result of non-technical employees misunderstanding examiner information requests and not understanding the NIST 800 control series
    d. This tool can either replace or augment regulatory cyber examinations and help examiners focus their attention on the subject's regulatory shortfalls identified by the tool
10. Producing a written report to prove technological compliance does not comport with Sarbanes Oxley (SOX) or AICPA audits
    a. There is no audit trail possible with documents containing subjective noisy text[18]
    b. There is no ability to produce risk metrics from documents or subjective noisy text
    c. The commercial GRC tools do not perform any of the functions I am suggesting in this proposal
    d. Most regulatory examinations focus on written documentation specifically produced for the examination
11. Regulatory cybersecurity compliance requires personal accountability:
    a. GDPR Article 42[19] and 43[20] detail a future Cybersecurity certification scheme
    b. It is six years since the EU released their final report on their Study of Articles 42 and 43 Data Protection Certification Mechanisms[21]
    c. The EU still has not identified a certification program, likely for the same reasons that the DoD's CMMC-AB will be performing their ISO certifications of C3PAO's themselves[22]
12. There could be record level security so that only escalations that have breached a set regulatory threshold could result in a notification to DHS and/or Regulators
    a. Respecting the 4th Amendment, this notification to DHS or a Regulator would only unlock the data relevant to an issue under their supervision
13. This system could also be capable of providing metrics on sensitive and privileged staff attrition, especially those that have access to CUI
    a. This tool could be used to compile a lot of metrics that would be useful for the Department of Commerce, DHS and Regulators
14. If the CMMC program will expand beyond the DoD as DHS has suggested, this tool could also be used to notify the CMMC-AB who needs to go through CUI training[23] and prospectively identify those who need to be licensed as CMMC Practitioners[24] or Assessors[25]
15. The critical infrastructure private sector primarily relies on non-technical resources in GRC roles to in accordance with the COSO Enterprise Framework (COSO):

a. COSO is commonly known as the *Three Lines of Defense* which segments functions into different C-level reporting structures:
    i. Operations, IT and cybersecurity is the first line (1LOD)
    ii. Compliance and Risk including third party, IT, cyber and operational risk is the second line (2LOD)
    iii. Audit is the third line (3LOD):
b. The Treadway Commission created the COSO Enterprise Framework in 1992[26] as a result of the Savings and Loan crisis where 1,043 savings banks failed
c. COSO's purpose is to combat corporate fraud by standardizing accounting controls, financial statements, bookkeeping, auditing and organizational structure
d. Regulators, external auditors and private sector institutions rely on COSO to measure technological and cyber risk even though it predates commercial use of the Internet
    i. I understand the theory behind COSO and how it is relevant and necessary for financial reporting, but I do not think it is appropriate for technology
    ii. I also appreciate that COSO and CPA's stepped up to fill a gap in technological assessments when no other option existed
    iii. At this point in our cybersecurity maturation and threat landscape, technology needs to be measured by technology and experienced technologists
e. AICPA (American Institute of Certified Public Accountants) standards also require COSO and for this reason CPA's perform SOC 2 audits
    i. I understand that the SEC requires Cybersecurity statements in public company Annual Reports, so I recognize that CPA's will have to remain involved in attesting to the integrity of the reporting in this tool, such as they do with financial reporting, but this tool could make it easier for them
    ii. I am not suggesting doing away with SOC 2's, as they are a very worthy exercise to help maturing organizations understand their deficiencies
    iii. I have managed SOC 2's with very technical CPA's who also had Computer Science degrees
    iv. Please recognize that I am not criticizing CPA's whatsoever, I am solely questionning the applicability of the COSO 2LOD Framework to measuring technological risk and compliance
f. COSO does not appear to require technical expertise for the 2LOD
g. COSO also allows the private sector to determine their own "Risk Appetite"
    i. The critical infrastructure private sector infers that this appetite allowance provides the latitude to ignore FISMA and the NIST 800 control series, possibly because both LOD is unaware of regulations
    ii. This proposed tool would solve that disconnect and do away with the need of having a 2LOD involved in cybersecurity and technology, except they could possibly receive reports produced by the tool as would the 3LOD
h. Perhaps some critical infrastructure institutions have a technically astute 2LOD risk function
    i. But my dominant experience is that the 2LOD is not technical, and putting non-technical resources in charge of assessing technical risk, creates risk instead of preventing it
    ii. When the 2LOD is non-technical, they rely on the 1LOD and 3LOD to self-identify technological risks, which are then manually entered into risk registers or regulatory documentation, but this process does not produce any meaningful risk posture because they are usually issues, not risks
    iii. This COSO structure in the private sector often results in Cybersecurity's resentment of the Risk and Compliance function because they don't understand the logic of having non-technical oversight that constrains their efforts and budget

	iv. In many institutions any commercial tool that serves a compliance function is automatically relegated to the 2LOD, but many commercial compliance tools are only relevant to highly trained technologists v. Most commonly the 2LOD risk functions do not have any viewing rights or API of any 1LOD System of Record ITSM inventory, permissions, change control, exception handling, vendor performance or CMDB and this renders risk assessments impossible 16. If the tool were to incorporate the NICE Framework as I have suggested previously it would also guide the critical infrastructure on their organizational structure and staffing qualifications a. This automation will enhance their cybersecurity posture, decrease risk, increase staff productivity, reduce costs and overhead 17. The Cyberspace Solarium Commission[27], under their Legislative Proposals (page 128) is recommending that SOX be modified to include that security control evaluations be performed by those with information security expertise 18. Jen Easterly, Director of Cybersecurity and Infrastructure Security Agency (CISA) at DHS appeared a Congressional hearing on September 23, 2021 about National Cybersecurity Strategy: Protection of Federal and Critical Infrastructure and testified that "*A modernized FISMA should shift the spotlight from compliance to risk management and implementation. This approach has led to an operating environment with heavy compliance requirements that do not always contribute to the intended outcome and in some cases distract from it. Instead, an environment that fosters implementation should ensure that cybersecurity actions enable agency missions and that agency leadership decisions appropriately prioritize and fund the security of their systems and networks*."[28] a. Given Director Easterly's background in the regulated critical infrastructure private sector, I am confident that she would agree that standardizing and automating the NIST CSF and 800 series is in our national best interest
SECTION 4 Attributes of the Proposed Solution to Enhance Supply Chain Risk Management	The NIST Supply Chain Risk Management guidance could also be turned into another feature of the tool: 1. Can potentially be built with existing no-code commercial software a. It will not involve uploading documentation nor divulging information that the Government is not already entitled to know 2. There can be two components of the tool, one is for vendors to complete their disclosure and the other is for the critical infrastructure private and public sector to identify their vendor inventory 3. Vendors could complete the NIST CSF/800 conformance tool from which they will receive a maturity grade 4. Vendors may still utilize external cyber consultants to help them operationalize their NIST 800 series conformance, but ultimately this tool will serve as a "One and Done" RFI for vendors, rather than have them go through lengthy questionnaires and discovery with each customer as they presently do a. It could significantly shorten their sales cycle and help the critical infrastructure qualify vendors 5. The questions can go into control detail but again, be captured in a structured format such as drop downs, check boxes and yes/no statements 6. The tool will comport to existing laws and regulations and derive data that vendors are contractually obligated to disclose and adhere to 7. The tool could measure vendor's product line adherence to the NIST 800 series and provide scoring a. Each vendor product can have to go through its own survey 8. The third-party risk survey tool can also focus heavily on attributes required to protect, store, process and manage CUI 9. The tool can ultimately be used for small vendors to qualify to sell to the critical infrastructure and perhaps grade them in their ability to handle or process CUI 10. Vendors could have to disclose all of their third parties, both technological, channel and services

11. Vendors could have to disclose any subcontracts and their input could remain in an incomplete pending status until their subcontractors complete their own disclosure too (as a separate entity)
12. Vendors could have to disclose their current customers, their supply chain and data sharing partners which perhaps may be solely viewable to the GSA and agencies involved in their procurement
    a. According to the GAO this disclosure establishes a vendor's qualifications
    b. This data also prevents a conflict of interest
    c. It could also be used as a validation point for the critical infrastructure to see if their disclosure is complete and/or perhaps identify software in their environment that they are unaware of
13. Vendors could also have to disclose the identities of their privileged or cyber staff, their work locations and whether or not they work from home
14. The critical infrastructure public and private sector will complete a section in relation to CUI, identifying the vendors they use to manage CUI and then they can identify those with privileged access to the CUI
    a. This information can then be transmitted to the CMMC-AB and/or to DHS's CMMC equivalent to ensure that those with CUI access have gone through CUI training and certification
15. In addition to identifying systems that store or process CUI, there are FAR and Treasury regulations concerning Third Party Risk, and this system can distinguish between legal requirements and guidance, but ultimately produce a risk score for both the vendor and customer
16. Depending upon the score, then DHS can perform additional discovery
17. Traditionally privileged access is measured by examiners as a single process across an institution, yet privileged access techniques differ depending upon the system being administered
    a. Some commercial software privileged access can be configured with rules
    b. Some managed services are outsourced and may not follow a customer's privileged access policies despite being contractually obligated to

SECTION 5

Business Case of the Proposed Solution to Enhance Supply Chain Risk Management

1. It is not reasonable to expect anyone except those with deep knowledge of technology, regulations, financial reporting, and AML/KYC investigations to be able to perform third party risk assessments
    a. If Supply Chain Management was centralized it would enhance the private sector's ability to focus their investment on growing their core business
    b. The private sector cannot be expected to break open devices and inspect components down to the chip level, but it is not possible to sufficiently perform third party risk assessments without this insight
2. The Federal Government struggles with performing third party risk assessments, thus the CMMC and FedRAMP[29] program
3. I have decades of experience in tech, and while I excel at qualifying technology, at times I struggle to identify investors of entities owned by private equity or foreign corporations
    a. Federal guidance[30] suggests that privately owned vendors should file SEC Form D[31] before selling to the critical infrastructure, yet very few do
    b. I have never seen any commercial Third Party Risk software or questionnaire delve into vendor ownership structure sufficiently, but this disclosure is also required by the Patriot Act[32]
    c. Perhaps a vendor's ownership and investment structure could be cross-checked on Treasury Edgar filings and databases before the vendor is able to use this proposed tool
        i. 2020 NDAA's Corporate Transparency Act[33] will result in Treasury producing a Federal Database of Beneficial Ownership Information of privately held corporations by 2023
        ii. The Holding Foreign Companies Accountable Act PCAOBUS maintains a list[34] of companies that do not comport to SOX, but they do not yet maintain a list of foreign nation state involvement
    d. The goal of these Treasury regulations is to prevent adversarial foreign access to CUI, so if the tool incorporates these functions it could possibly prevent attacks and data leakage
    e. Any changes in beneficial ownership could be identified by vendors filing a SEC Form 4[35] which is then circulated by the vendor to their customers through this tool at least 90 days before the closing of the investment or sale

f. Reporting changes in beneficial ownership would give customers time to file an objection to the sale, or the ability to secure their data and exit their contracts if the change presents a conflict of interest, a violation of their regulatory or contractual obligations or a threat to their business, such as in the case of their vendor being acquired by a direct competitor or affiliated with a sanctioned nation state

4. This tool would not replace FedRAMP, but perhaps be complimentary, as it would not certify vendors, it would only serve as a legal attestation of their present NIST CSF and 800 series disclosures
5. This will make it easier for SMB vendors and emerging technologies to compete for contracts in the Federal Government and the critical infrastructure private sector because they will be able to identify vendors suitable for their line of business
6. This tool can also be used to identify emerging vendors who may have very desirable technology, yet do not yet have the income to secure their operations sufficiently
   a. The critical infrastructure completing their vendor inventory, can either select from the drop down and pre-populated list of vendors will appear, but if they add a new vendor then the vendor could automatically be prompted to complete the NIST CSF disclosure themselves
   b. If the new vendor is not qualified to handle CUI, yet their technology is disruptive and in the U.S. national interest, they can be steered to public and private programs that can help with CUI certifications, funding and grants

SECTION 6

Proposed Solution Caveats, Comments and Exceptions

1. This NIST automation solution will NOT replace the need for GRC systems or Security Consultants
   a. Commercial GRC tools capture issues and risks that are often related to escalations, projects, change control, exception management and expired data or end-of-life technology
   b. This NIST tool could be developed in-house by NIST as to avoid any conflict of interest
2. This tool would likely increase NIST NCCoE[36] membership and feedback
3. There could be a phased implementation by industry sector
4. This tool can aid the DHS CISA and other agencies to create strategies to stop large scale attacks
   a. Presently CISA has an idea about the greatest single points of failure, but with this tool they will have empirical data that they can use to formulate defensive measures
   b. If a critical infrastructure public or private sector institution is attacked, presently Federal LEO requires manual notification after the event, and even then the Government is not aware of what systems were affected or the attack vector
5. President Obama's Executive Order 13556[37, 38] is the least known or understood law in the United States
   a. This law is fundamental to protecting the critical infrastructure information security
   b. If the critical infrastructure does not know about this law, they have no way of designing a sufficient cybersecurity program to protect their CUI
   c. Perhaps this tool can start off by requiring agency examiners, the critical infrastructure private sector C-Level and Board of Directors (BOD) to go through industry specific CUI and FISMA training and pass a test before the rest of the tool can be completed
   d. This way the C-Level and BOD will understand why they then receive alerts of non-compliance
   e. I have witnessed institutions spend far more on the appearance of compliance, rather than just complying and I believe this is due to lack of knowledge about CUI and FISMA
   f. This system could be used by institutions to identify their CUI and also ensure that it is marked and protected accordingly
   g. It could eventually become a CUI Access Registry, which I believe was President Obama's original intention with the Rockefeller Snowe Cybersecurity Act[39]
6. The tool could disallow contractors and consultants from completing it for customers
   a. Any contractors or consultants should have to complete their own survey if supporting or selling to the critical infrastructure private sector
7. If this tool was implemented by NIST it could probably be prototyped within months, whereas standing up a new technological licensing agency would probably take over a decade

8. President Obama's November 2010 Executive Order 13556 -- Controlled Unclassified Information was likely the result of the Rockefeller Snowe Cybersecurity Act of 2010 failing in Congress
    a. In 2012 Senator Rockefeller referred to ongoing critical infrastructure cyber attacks by foreign nation states as warfare and the greatest national security risk facing the U.S.[40]
    b. Everything contained within that 2010 Cybersecurity bill is now coming to pass thanks to the Cyberspace Solarium Commission, DHS CISA, the NDAA and Presidential mandates
    c. Yet 12 years have passed and the private sector still doesn't know what CUI is
    d. We likely could have avoided many of the large scale breaches if the CUI laws were enforced
        i. We cannot implement any meaningful cybersecurity without first upholding the basic law underpinning all data protection, Executive Order 13556
9. This tool could also provide Regulators with insight on critical infrastructure attrition, outsourcing and offshoring
    a. High cybersecurity staff turnover is an existential threat
    b. Cybersecurity attrition is often an examination measurement
    g. In my experience Cybersecurity staff often leave for these reasons:
        i. They identify a breach or data leakage and are terminated for doing so
        ii. They identify serious gaps in their cyber hygiene that leadership refuses to remedy
        iii. They recognize that if a breach takes place while they are employed, it can damage their career
10. There would be some overlap between these two proposed systems
    a. Such as in the case of privileged access management, I see that controls pertaining to the vendor commercial solutions may differ depending upon the system
    b. Just because a vendor's solution has GRC functionality, it is often an optional feature that requires configuration by the system administrator, so this NIST tool could seek how the Vendor's tools address controls, but also whether their customers have implemented these features
    c. If the vendor stores or processes CUI, then those with privileged access to the vendor's environment could be identified and any changes in staffing alerted to leadership and Regulators if attrition meets certain thresholds
11. When I come across willful violation of data protection laws, the decision to do so is often out of ignorance, where an employee or vendor is solely focused on protecting their self-interest
    a. Many times it is out of desire to preserve their contract, headcount and reporting structure, because manual process requires more staff than automation
    b. I do not believe that any CEO or Board of Directors wants to add cybersecurity risk to their business, but they do not yet have an automated method to become apprised of risk
12. Benjamin Lawsky, the father of NY State Department of Financial Services Cybersecurity law 23 NYCRR 500 said "I think if I look back, the one thing I wish we had done earlier was shifted to a focus on individual accountability. Large fines will only get you so far, especially because a lot of that is just being handled by shareholders. If you hold individuals accountable, I think that is really when you are going to see a change in conduct."[41]
13. CUI laws are to protect data that can impact our national security, including PII[42]
    a. Existing CUI laws are more protective than any State or Foreign Privacy laws such as CCPA and GDPR
    b. If CUI were upheld and enforced it would likely negate the need for CCPA and offer even greater protection to consumers and businesses than any State data privacy law
        i. Instead we are putting great financial pressure on American businesses to comport to CCPA and other State privacy laws which will erode profits and not offer any real protection to consumers
        ii. If CUI laws were upheld it would also secure many other business sectors outside of the critical infrastructure

iii. If CUI laws were upheld it would devalue data brokers, thereby reducing the financial incentive to attack American businesses and institutions

c. Consumers and employees are the conduit to Nation State attacks

d. A compromised employee is a compromised employer

e. Our critical infrastructure security posture is very precarious and the quickest way to solve this is to uphold President Obama's CUI mandate now, this should be our national priority[43]

14. If CUI laws were enforced then complying with the NIST CSF and securing our Supply Chain will not be difficult

a. Both the NIST CSF and Risk Management Framework (RMF) are often ignorded by the critical infrastructure private sector because neither is possible without identifying all of the violations and risks presented by not adhering to CUI laws

i. It would cause much legal exposure for those with CUI to memorialize data flows and map it to inventory, persons, contractors and partners

ii. But how can you protect anything unless you first identify what you have, where it is and who has access to it?

b. This crisis reminds me of the 2001 dot-com bubble and the subprime mortgage financial crisis, many recognized the damage it was causing but no one in a position of authority had the will to stop it

i. We are in a rapid cybersecurity maturation cycle and someone needs to identify the problems otherwise the alternative is too frightening to contemplate

c. **Data Privacy and Cybersecurity are not mutually exclusive. Neither is possible without the other.**

SECTION 7

Citations

1. Supreme Court Cites NIST Mobile Forensics Guide in Ruling on Cell Phone Searches https://www.nist.gov/news-events/news/2014/07/supreme-court-cites-nist-mobile-forensics-guide-ruling-cell-phone-searches
2. FIPS 199 Federal Information Processing Standards Publication - Standards for Security Categorization of Federal Information and Information Systems https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.199.pdf
3. Sarbanes Oxley Act of 2002 https://www.govinfo.gov/content/pkg/COMPS-1883/pdf/COMPS-1883.pdf
4. Fiscal Year 2021-2022 Guidance on Federal Information Security and Privacy https://www.whitehouse.gov/wp-content/uploads/2021/12/M-22-05-FY22-FISMA-Guidance.pdf
5. FAR Part 9 - Contractor Qualifications https://www.acquisition.gov/far/part-9
6. FAR Part 16 – Types of Contracts https://www.acquisition.gov/far/part-16
7. DFARS Part 232 - Contract Financing https://www.acquisition.gov/dfars/part-232-contract-financing
8. Holding Foreign Companies Accountable Act https://www.congress.gov/bill/116th-congress/senate-bill/945/text
9. Holding Foreign Companies Accountable Act – Morrison and Foster Client Alert 08 Dec 2020 https://www.mofo.com/resources/insights/201208-holding-foreign-companies-accountable-act-chinese-companies.html
10. Controlled Unclassified Information (CUI) Registry - https://www.archives.gov/cui
11. NICE Framework Categories, Work Roles, Competencies, Tasks, Knowledge and Skills https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center/workforce-framework-cybersecurity-nice
12. COSO Enterprise Framework – September 29, 2004 https://www.coso.org/pages/erm-integratedframework.aspx
13. SEC Proposes Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies https://www.sec.gov/news/press-release/2022-39
14. Federal Information System Controls Audit Manual (FISCAM) https://www.gao.gov/assets/gao-09-232g.pdf

15. Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf
16. Executive Order on Improving the Nation's Cybersecurity - May 12, 2021 https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/
17. CUI Category: Information Systems Vulnerability Information https://www.archives.gov/cui/registry/category-detail/info-systems-vulnerability-info.html
18. Noisy Text definition https://www.techtarget.com/searchbusinessanalytics/definition/noisy-text
19. GDPR Article 42 – Certification https://gdpr-info.eu/art-42-gdpr/
20. GDPR Article 43 – Certification Bodies https://gdpr-info.eu/art-43-gdpr/
21. European Commission Data Protection Certification Mechanisms Study on Articles 42 and 43 of the Regulation (EU) 2016/679 https://ec.europa.eu/info/sites/default/files/data_protection_certification_mechanisms_study_final.pdf
22. C3PAO CMMC Third-Party Assessor Organization https://cmmcab.org/c3pao-lp/
23. DoD Mandatory Controlled Unclassified Information (CUI) Training https://securityawareness.usalearning.gov/cui/index.html
24. CMMC Practitioner https://cmmcab.org/registered-practitioners/
25. CMMC Professional or Assessor https://cmmcab.org/assessors-lp/
26. The Committee of Sponsoring Organizations' (COSO) history https://www.coso.org/Pages/aboutus.aspx
27. Cyberspace Solarium Commission https://www.solarium.gov/
28. Testimony Jen Easterly, Director Cybersecurity and Infrastructure Security Agency, DHS on a Congressional hearing for "National Cybersecurity Strategy: Protection of Federal and Critical Infrastructure Systems" https://www.hsgac.senate.gov/imo/media/doc/Testimony-Easterly-2021-09-23.pdf
29. FedRAMP Mission, Benefit and Goals https://www.fedramp.gov/program-basics/
30. Proposed Interagency Guidance on Third-Party Relationships: Risk Management https://www.fdic.gov/news/press-releases/2021/pr21061a.pdf
31. SEC Form D https://www.sec.gov/about/forms/formd.pdf
32. Patriot Act https://tinyurl.com/2wr35ckv
33. Corporate Transparency Act https://www.congress.gov/bill/116th-congress/house-bill/2513/text
34. Audit Reports Issued by PCAOB-Registered Firms Located Where Authorities Deny Access to Conduct Inspections https://pcaobus.org/oversight/international/denied-access-to-inspections
35. SEC Form 4 https://www.sec.gov/files/form4.pdf
36. NIST National Cybersecurity Center of Excellence https://www.nccoe.nist.gov/
37. Executive Order 13556 -- Controlled Unclassified Information – November 2010 https://obamawhitehouse.archives.gov/the-press-office/2010/11/04/executive-order-13556-controlled-unclassified-information
38. CUI Notice 2020-01: CUI Program Implementation Deadlines – May 2020 https://www.archives.gov/files/cui/documents/20200514-cui-notice-2020-01-cui-program-implementation-deadlines.pdf
39. S. 773 (111th): Cybersecurity Act of 2010 - https://www.govtrack.us/congress/bills/111/s773
40. Senator Rockefeller speaking about cyber warfare by nation states against the U.S. – March 2012 https://www.c-span.org/video/?304936-1/communicators-senator-jay-rockefeller
41. Ben Lawsky: We should have done this earlier – May 2015 https://www.cnbc.com/2015/05/26/ben-lawsky-we-should-have-done-this-earlier.html
42. CUI Category: General Privacy - https://www.archives.gov/cui/registry/category-detail/privacy.html
43. OMB - Preparing for and Responding to a Breach of Personally Identifiable Information – January 2017 https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2017/m-17-12_0.pdf