Securing Systems Against Modern Threats

A Case for Zero-Trust Cybersecurity Architecture

Nathaniel Furman

Institute of Electrical and Electronics Engineers

Summer 2021

WISE WASHINGTON INTERNSHIPS for STUDENTS of ENGINEERING

IEEE

MIAMI COLLEGE of ENGINEERING

What we should actually be doing is thinking about what are our key controls that will mitigate the risks. How do we have those funneled and controlled through the team that we have, how do we work through that in a well formatted, formulated process and pay attention to those controls we have chosen?

Dr. Chris Pierson

Table of Contents

Executive Summary

With the exponential rise of digital devices and systems, a mirrored rise in cyber threats in the United States occurred. Successful or not, these attacks pose a serious risk to every citizen. Data breaches have harmed and will continue to harm the livelihood of millions of Americans through targeted harassment, stolen funds, ransomware, and more. It is not difficult to find reports in any given month of a significant cyberattack. Recent incidents include the attacks on Colonial Pipeline, Equifax, and SolarWinds [28-30].

Current legislation and enforcement are ineffective. With the Privacy Act of 1974 drawing attention to data security, and passage of the first Federal Information Security Modernization Act (FISMA) in 2002, it is clear the U.S. government tried to address cybersecurity for decades. More recently with the 2014 FISMA revision and establishment of the Cybersecurity and Infrastructure Security Agency (CISA) under the Department of Homeland Security (DHS) in 2018, the U.S. government has fully recognized the growing threats to information technology (IT) systems [8].

Even with the 2014 FISMA, compliance has been inconsistent at best with many federal agencies continuing to be non-compliant – the Office of Personnel Management (OPM) provides a clear example [27]. The agency's weak IT infrastructure remained non-compliant for years prior to its 2015 data breach. Attackers compromised millions of fingerprints, Social Security numbers, and other significant personally identifiable information of both public and private individuals possessing top-secret clearance. Now, more than five years after the breach, audits by the OPM's Office of the Inspector General (IG) show continuing FISMA non-compliance.

Cybersecurity threats also changed since the introduction of FISMA, particularly with the rise of the Internet of Things (IoT) and connected devices. Classic models of perimeter-based network defense are insufficient within a remote and wide-reaching organization [37]. New models must be introduced and implemented with continuing improvements in IT systems.

The following recommendations strive to address the strengthening of U.S. cybersecurity and network infrastructure for modern threats and systems. One solution may help, yet cannot repair the problems resulting from employment of weak IT systems over many years without substantial resources spent to deter, detect, and prevent cyberattacks. With the implementation of multiple recommendations, Americans may be able to restore their faith in government protections and security of their personal information.

1) **Improved FISMA enforcement**

   FISMA enforcement should be improved through funding allocations and improved audits. In the current FY2022 Department of Homeland Security appropriations bill, increased funding for CISA mission support activites and specifically audits should be allocated. Through the DHS and CISA, audits of IT systems should be undertaken more frequently and thoroughly.

2) **Revise NIST Special Publication 800-207**

   The National Institute of Standards and Technology's (NIST) Special Publication (SP) 800-207 on Zero Trust Architecture (ZTA) should be revised in a few key areas. These include legacy system information, deployment cases, and user responsibilities. Integrating older systems with new technology and agency regulations is a significant challenge, but one that can be achieved through thoughtful revisions. The deployment cases and use cases described in this publication are limited and lack the detail many agencies will find useful. The NIST Information Technology Laboratory (ITL), who is responsible for the 800 series of publications, should solicitate revisions and release an updated publication.

3) **Allocate funding for IT services and small businesses**

   Through CISA or Congressional budget allocations, a consulting service for small businesses should be implemented in CISA. With too many local and state level IT systems vulnerable to cybersecurity threats, increased funding for IT services across the U.S. government will help mitigate future threats. Smaller contractors and businesses are also at higher risk, with as many as 44 percent of cyberattacks targeting small businesses yearly. Implementing a consulting or partnership service to help small businesses access to resources commonly available to larger entities is essential for better threat prevention.

4) **Require mandatory reporting**

   Requiring all U.S. government agencies, contractors, and critical infrastructure companies to report significant cybersecurity incidents – from data breaches to system attacks – will help contain possible damage and help ensure the accurate and effective mitigation of future attacks. Setting a proper timeline, procedure, and response policy are needed for an effective system.

The federal government is responsible for ensuring the availability of effective cybersecurity public policies. With these recommendations, a stronger cybersecurity infrastructure is achievable for current and future information systems.

Foreword

About the Author

Nathaniel Furman graduated from the University of Miami in May of 2020 where he earned a B.S. in electrical engineering with a second major in physics. At the University of Miami, Nathaniel was active in IEEE and served as president of the IEEE honors society Eta Kappa Nu (HKN) his senior year. Nathaniel is currently pursuing his Ph.D. at the University of California, Irvine under Dr. Filippo Capolino with a focus on slow-light photonics and electromagnetic theory. His interests include information security, cognition, terahertz devices, and photonics.

About the WISE Program

The Washington Internship for Students of Engineering (WISE) program was founded in 1980 through the collaborative efforts of various professional engineering societies. During its successful run, this program has become one of the premier Washington internship programs. Each summer, participating societies select exemplary students in engineering or computer science programs who are nearing completion of their undergraduate degree or are recent graduates. These students are selected from a national applicant pool and work closely with their sponsoring society during the nine-week program. By gaining exposure to policymaking through leaders in the Federal Government, students are responsible for researching, writing, and presenting a paper on a topic pertinent to their sponsoring society. For more information about the WISE program, please visit www.wise-intern.org.

About IEEE

The Institute of Electrical and Electronics Engineers is the world's largest technical professional organization dedicated to advancing technology for the benefit of humanity. Built on the core values of trust, growth, global community building, partnership, service to humanity, and integrity in action, IEEE's over 400,000 members in more than 160 countries continue to inspire the next generation of learners. IEEE includes over 500 affinity groups, over 30 technical societies, and over 5.3 million publications.

Acknowledgments

I would like to thank the entire WISE team and the IEEE-USA office for the opportunity to participate in this program. A special thanks to Erica Wissolik for coordinating WISE and Diana Librizzi for introducing me to the program and encouraging me to apply. I would like to acknowledge Mark Ames as our faculty member-in-residence. I am deeply grateful for the conversations with policy experts throughout the summer. Finally, I would like to thank the entire WISE cohort for their advice, support, and resilience in participating from around the country due to Covid-19.

Acronyms

CIO	Chief Information Officer
CISA	Cybersecurity and Infrastructure Security Agency
DHEW	Department of Health, Education, and Welfare
DHS	Department of Homeland Security
DoD	Department of Defense
EO	Executive Order
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Modernization Act
FITARA	Federal Information Technology Acquisition Reform Act
GAO	Government Accountability Office
IEEE	Institute of Electrical and Electronics Engineers
IG	Inspector General
IoT	Internet of Things
IT	Information Technology
ITL	Information Technology Laboratory
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OMB	White House Office of Management and Budget
OPM	Office of Personnel Management
OSHA	Occupational Safety and Health Administration
RMF	Risk Management Framework
SP	Special Publication
VA	Veterans Affairs
ZT	Zero Trust
ZTA	Zero Trust Architecture

Table of Figures

Introduction

For as long as information storage existed, our protection of it has been increasingly important. Since the creation of the first digital storage device in 1947 [1], we have followed Moore's Law to reach incredibly high volume and affordable storage today. With an estimated 10 to 15 exabytes (one million terabytes) of data in one company's hands [2], the need for better information security is required now more than ever.

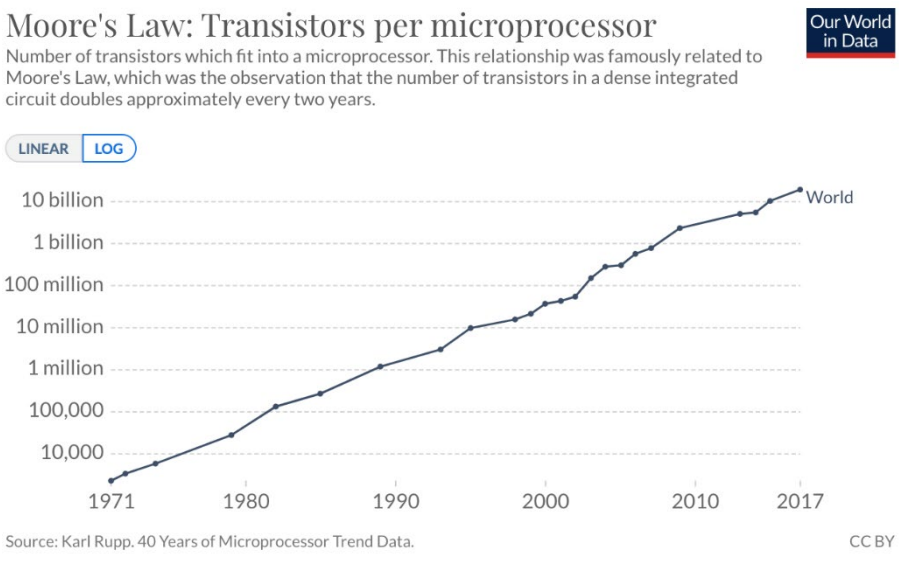

Figure 1. Moore's Law visualized [54].

The cost of failure is also increasing. As described by IBM Security in their 2020 report [3], the average total cost of a data breach in the United States exceeds $8.64 million. With an increase of more than five percent from the previous year, this upward trend is expected to continue. However, IBM's study examined only corporations rather than federal agencies such as Department of Veterans Affairs (VA). The VA hospitals are part of the most targeted industry for cyberattacks. When including data breach costs from the government sector, it is even more pertinent to improve cybersecurity systems.

Successful attacks are primarily a result of human error rather than software vulnerabilities [4]. Although human error can take many forms, simple solutions in system infrastructure can mitigate large scale data breaches. Either from users or administrators, improper configurations or shortcuts taken during work, a single error cannot be allowed to dismantle or compromise an entire network. Careful implementations of *segmented systems* following zero trust

Segmented systems – n., a virtual process that creates address spaces of various sizes in a computer system, called segments. Each segment is a different virtual address space that directly corresponds to process objects. When a process executes, segmentation assigns related data into segments for faster processing. The segmentation function maintains a segment table that includes physical addresses of the segment, size, and other data.

architecture principles is the solution. However, the question is not if data breaches will happen – the question is how we can effectively mitigate the risks.

By implementing the recommendations described here, the effects of a single system breach may be significantly reduced across U.S. Federal agencies and corporations. This will effectively reduce the cost per data breach, encourage better cybersecurity practices, and compartmentalize systems into manageable segments. Individual errors will not be able to compromise an entire network.

This paper describes the information important to understanding the motivation and background of U.S. information system security. This paper will also describe current system requirements and recommendations along with factors influencing the vulnerability of cybersecurity systems. Recommendations moving forward will be presented in detail, with discussion of effectiveness and ease of implementation.

1. Background

To understand both these policy recommendations and motivation for minimizing human error in IT systems, a brief yet foundational background is important. This section describes current legislation influencing U.S. information technology (IT) system implementation and the structure of standards and enforcement.

1.1 History of information security

While entire textbooks can be written on the history of information security, this section gives an overview of important legislation relating to modern digital storage and access systems. It is first useful to define an information system, data storage system, or IT system, which will be used interchangeably for the purposes of this paper. Encyclopedia Britannica defines an information system as “an integrated set of components for collecting, storing, and processing data and for providing information, knowledge, and digital products” [5]. In other words, information systems manage the storage and retrieval of data.

Perhaps the first piece of legislation impacting current systems is the Privacy Act of 1974. As a result of Watergate and in an effort to restore trust in the government, a report from the then Department of Health, Education, and Welfare (DHEW) described risks to privacy from the increasing use of electronic IT systems. Using this report as a backbone for the 1974 act, Congress established a Code of Fair Information Practice for the collection, retention, and disclosure of an individual’s records.

The DHEW report was instrumental in early national and international cybersecurity policies and legislation [6]. Using a “code of fair information practices”, the authors of the report set the foundation of our current system which uses, in part, Federal Information Processing Standards or FIPS.

For context, one of the authors of the DHEW report is recognized as the founder of the field of information security and would find critical vulnerabilities in the then called ARPANET (now Internet) [7].

More recently, Congresses passed two key 2014 acts focusing on IT security and management. The Federal Information Security Modernization Act of 2014 (FISMA) establishes roles and responsibilities for federal agency information technology security [8]. Broadly, this revision of the original 2002 act gives more power to the White House Office of Management and Budget (OMB) and requires agencies to implement standards set by the National Institute of Standards and Technology (NIST). The organizational hierarchy set by FISMA is described in the next section.

The second act, The Federal Information Technology Acquisition Reform Act of 2014 (FITARA), expands the role of Chief Information Officers (CIOs) in managing IT investments [9]. With this act, CIOs have increased oversight in IT acquisitions and work closer with the OMB for IT investments and risk management.

In addition to these two cornerstone acts, a few other important and recent federal documents have been published. This includes the NIST Special Publication (SP) 800-53 on Security and Privacy Controls for Information Systems and Organizations (rev. 5, Dec. 2020) and Executive Order (EO) 14028 on Improving the Nation's Cybersecurity (May 2021) [10][11]. NIST released the first version of SP 800-53 in December of 2006, and previous administrations have discussed many topics in EO 14028 for years [12]. These actions illustrate the importance of information security to the U.S. government.

The Cybersecurity and Infrastructure Security Agency Act of 2018 established the Cybersecurity and Infrastructure Security Agency (CISA), a resource for U.S. agencies and other federal systems. While CISA along with the previously discussed laws, publications, and executive orders influence implementation of protections for current IT systems, many U.S. agencies retain partial autonomy over their systems. For instance, the VA manages the IT systems between their network of hospitals [13].

More specifically related to zero trust (ZT) systems, the Defense Information Systems Agency and the Department of Defense (DoD) published their work on a "black core" enterprise security strategy in 2009. Taken with the work of John Kindervag in 2004 on the de-perimeterization of IT systems, the foundations of ZT systems were created [15]. Section 2.1 discusses ZT systems and zero trust architecture (ZTA) in detail.

About CISA:

CISA publishes, maintains, and helps distribute/integrate its National Cybersecurity Protection System available for the Federal Civilian Executive Branch and other federal entities. CISA can also provision additional technical capabilities for improved security and threat detection [14]. This agency contains the technical core and expertise for U.S. cybersecurity moving forwards.

Although information security has been detailed, documented, and discussed for many decades, this background provides an overview of legislation relating to IT systems and security. From the adoption of computer systems by the federal government to recent EOs, this topic is constantly changing and evolving. The revisions, discussions, and context for much of the legislation described above could not be effectively addressed in this brief background. The references following this paper provide additional information and context.

1.2 Current organizational hierarchy and standards

Two documents which describe the authority and hierarchy of current federal information systems are FISMA and OMB Circular A-130. FISMA (2014 revision) establishes the roles and responsibilities for federal agency IT security and OMB Circular A-130 establishes general policy for the programming, planning, budgeting, and execution of federal IT resources [8][16]. The organizational system described by the following text originates from these two documents.

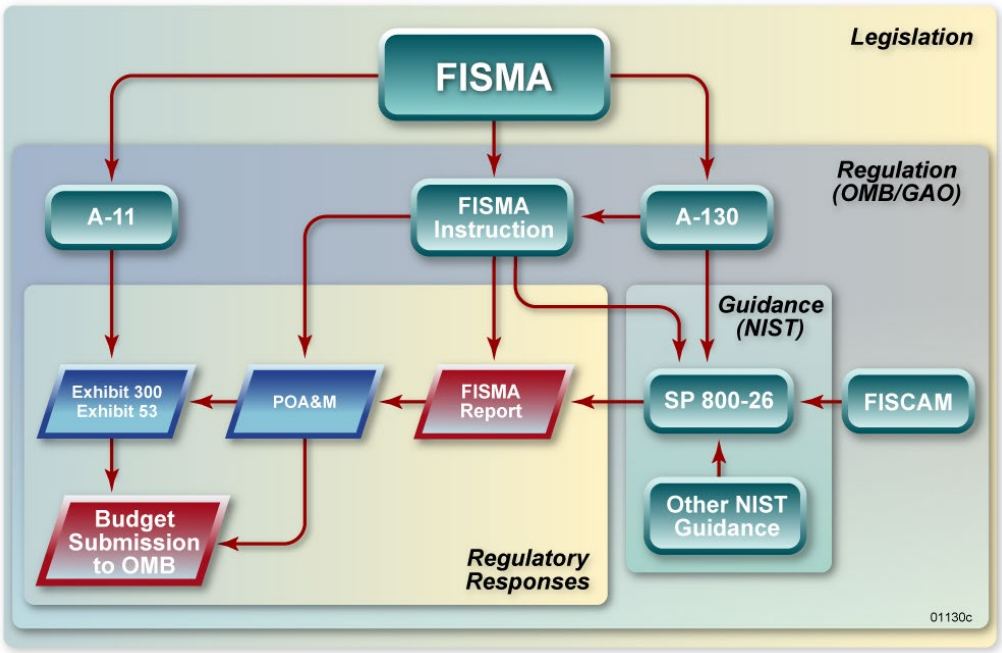

Figure 2. FISMA organizational hierarchy [42].

While agency heads are ultimately responsible for IT security, they may delegate responsibilities. Even with partial autonomy, every agency must follow guidance issued by the OMB and standards published by NIST when implementing their IT systems. This structure is shown in Fig. 1. It should be noted that SP 800-26 (Security Self-Assessment Guide for Information Technology Systems, 2006) is superseded by FIPS 200 (2006) and SP 800-53 (2020), both published by NIST and detailed further in the Appendix [10][18].

The DHS is also authorized to help agencies comply with OBM and NIST publications. As part of this compliance, each agency head or inspector general must produce an annual cybersecurity report. SP 800-53 (Security and Privacy Controls for Information Systems and Organizations) outlines an exhaustive list of suggested security controls possible for FISMA compliance [10].

More recently, agencies have been encouraged to use services provided by CISA in their IT security framework. For example, the Department of Veterans Affairs Office of the Inspector General recently reported on the risks in VA systems [19]. These risks may be mitigated and reduced by CISA cybersecurity provisioning as suggested in a recent Congressional Research Service (CRS) report [13].

In addition to NIST standards, the DHS may issue Binding Operational Directives (BODs) for federal agencies to implement. With the purpose of protection and security of federal information and IT systems, these directives are mandatory for federal agencies under FISMA with notable exceptions for national security systems. At an

agency level, additional policies, standards, and directives may be issued by the director or CIO. These may include contract security handbooks, reporting procedures, and more.

An overview of a few key NIST publications and DHS BODs referenced later in this paper can be found in the Appendix.

2. Current Regulatory Environment

This section will describe the effects of current regulations with an emphasis on system weaknesses and their effects. While significant legislation such as FISMA and FITARA, or important standards like SP 800-53 have improved IT systems at many agencies, too many vulnerabilities continue existing that should be mitigated with targeted solutions. This section specifically investigates how segmented and ZT systems reduce the risk of large cybersecurity breaches.

2.1 Defining zero trust systems

Before providing the NIST definition of a ZT system and ZTA given in SP 800-207, it is helpful to understand the now outdated prevailing security approaches. In these approaches, an agency or organization focuses on perimeter defenses. This includes but is not limited to a firewall or air-gaped system (a system not directly connected to outside networks). For some applications and organizations, this model is sufficient and effective. For example, it is common for data servers to have a secure physical perimeter and equally secure or more secure network firewall.

These perimeter-based systems are not without their flaws. Particularly, lateral system movement is generally unhindered and perimeter definition is vague. In short, once the perimeter is compromised or breached in a traditional network system, attackers can extract significant amounts of data without further trouble. Every connected system needs to be as secure as every other because the entire architecture is only as strong as its weakest link, like the chain cliché. As an example of this drawback, the recent attack on Equifax's systems highlights what can go wrong. Through one insecure web portal, near unhindered lateral network movement inside Equifax's firewall became possible and was exploited.

Another drawback which has recently become more impactful is the vagueness of a system's perimeter. With enterprises operating several internal networks, remote offices, cloud services, and off-site workers, expanding and defining a perimeter becomes increasingly difficult. Additionally, the rise of Internet of Things (IoT) devices and personal networking devices (phones, watches, tablets, etc.) increases the attack surface of a network. The more trusted devices, the more points of attack.

Ultimately, perimeter-based networks rely on implicit trust based on network location and single, static defenses over a large network segment. Thus begins initial work in defining and developing the next steps in network security: de-perimeterization and ZTA. Federal interest in de-perimeterization began with the Defense Information Systems Agency and the DoD nearly two decades ago.

After the DoD report on “black core” enterprise security strategies, FISMA laid out guidelines and structure encouraging the move to ZT systems that do not rely on a single, secure, perimeter. With SP 800-207 published in August of 2020, ZT and ZTA were given clear definitions as follows [20]:

> *Zero trust (ZT) provides a collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services in the face of a network viewed as compromised. Zero trust architecture (ZTA) is an enterprise’s cybersecurity plan that utilizes zero trust concepts and encompasses component relationships, workflow planning, and access policies. Therefore, a zero trust enterprise is the network infrastructure (physical and virtual) and operational policies that are in place for an enterprise as a product of a zero trust architecture plan.*

In short, ZT systems and ZTA assume no implicit trust and treat the network as compromised or breached regardless of the current network status and is illustrated in Fig. 3. This type of network provides significant benefits to current systems and threats. Most notably, data breaches are significantly less likely and when they do occur, they cost significantly less. ZT systems achieve this benefit by hindering lateral movement in a system, requiring additional precautions in data access, and segmenting enterprise networks.

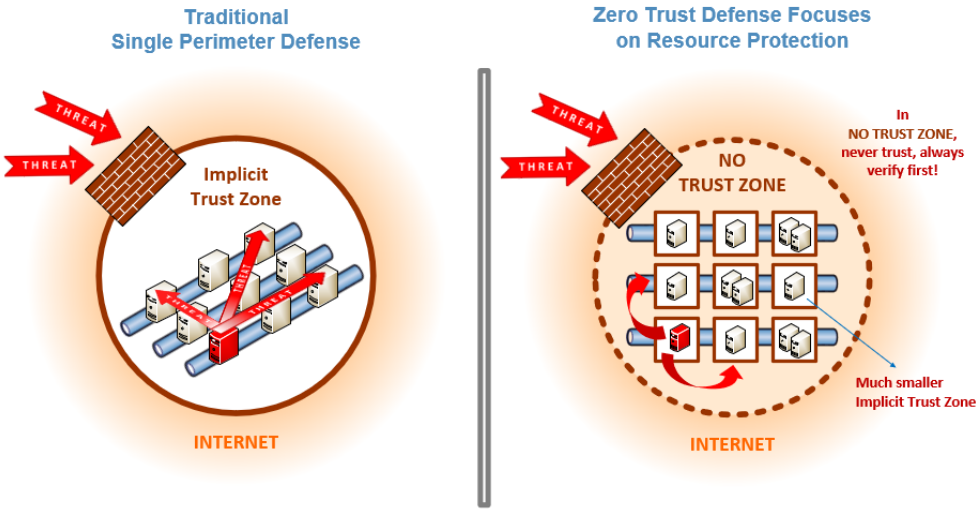

Figure 3. Zero-trust network comparison [47]

ZT systems and ZTA are not static definitions for every network. Depending on the sensitivity, risks, scale, and more, implementations of ZTA can vary in significant ways. For instance, the database of emails the Library of Congress uses for legislation updates requires different protections and standards than the Social Security Administration or the Internal Revenue Service.

2.2 Effects of current legislation

No legislation can entirely prevent a successful network breach. However, with sound policies and effective standards, FISMA, FITARA, and related legislation have significantly impacted U.S. cybersecurity systems in recent decades. As will be clear shortly, FISMA and FITARA have strengthened U.S. agency IT systems against malicious actors, both foreign and domestic.

FISMA was originally passed in 2002 and updated in 2014. While the Privacy Act of 1974 required U.S. agencies to protect personal information, this law lacked the detail FISMA was written to address. FISMA requires federal agencies and contractors to address 14 specific topics in their IT systems. These topics include access controls, incident response, system and communication protection, and more.

Throughout the history of FISMA, agencies have been updating their IT systems. The IG of each agency also releases an annual report detailing FISMA compliance. This includes weaknesses in cybersecurity infrastructure and suggestions for improvement. Thus, it is possible to track compliance and cross reference the IG reports with disclosed data breaches by agencies and contractors.

Through the IG reports, the effects of current legislation can be illustrated. Without detailing every agency or department, two examples are given that describe the findings from the IG reports and the changes in IT systems. The first example is from the Office of Personnel Management (OPM) and the second is from the VA.

As far back as 2007, and particularly between 2012-2015, IG audits of OPM networks described serious concerns in system implementation and FISMA compliance. OPM systems and databases did not meet criteria satisfactory to many of the domain areas reviewed. The reports were not all negative, with some NIST standards implemented for FISMA compliance. The 2020 IG audit of OPM shared a more promising outlook on IT systems. With an overall maturity level of “Defined,” this report shows improvements from the past five years, particularly in incident response and risk management. Although encouraging, the OPM has yet to implement several FISMA requirements in contingency planning and information security continuous monitoring; therefore, significant work remains for data protection and privacy [26].

The second example is from the VA. From its 2020 report, the IG’s office noted improvements in the centralization of control functions, better boundary protections and network threat monitoring techniques, a new governance, risk, and compliance tool, and more [19]. However, almost two decades after the first FISMA bill passed, the VA remains partially non-compliant in FISMA requirements. The IG noted many of the recently implemented controls need time to mature and demonstrate evidence of their effectiveness. Unfortunately, this time is something the VA and the veterans they serve may not have.

When discussing the impact of legislation, successful implementation is more difficult to track than unsuccessful implementation. This is especially true with cybersecurity systems where the less active the network, the better the system (in general). The difficulty of tracking the effectiveness of FISMA in thwarting possible attacks is compounded with the consistent rise of cyberattacks in the past two decades. These factors make it nearly impossible to determine with certainty FISMA's effectiveness. Nonetheless, it is clear that agencies and government contractors worked on steps to consider their IT infrastructure and IT security since the early 2000's.

2.3 Human error in information system breaches

As much as 88 percent of data breaches result from human error as found in a recent joint Stanford University and Tessian cybersecurity firm study [4]. Either as a direct or indirect consequence from any number of possibilities, the oversights, weak passwords, system configurations and more set by individuals have caused billions of dollars in damages with countless lives being affected. Without describing every way that human error compromises systems, this section will consider a few examples of recent breaches as a representation of data breaches in general.

As a first example, take a series of data breaches disclosed by the OPM in July of 2015 [27]. These breaches compromised the personally identifiable information of approximately 20 million American citizens, costing U.S. taxpayers an estimated half a billion dollars. These breaches are also more significant than the numbers might suggest due to the sensitivity of the data stolen. The OPM data breach contained the records of individuals entrusted with top security clearances with access to top secret information, providing an avenue for future, more severe, data breaches.

An interesting and unfortunate fact of this breach is the history of poor FISMA audits of the OPM. From 2012 to 2015, the IG's audits revealed serious gaps in IT security each year. Eleven of the internal systems operated without valid authorization requirements and attackers were able to move through the network after the initial compromised entry point. From the reports before and after the OPM data breach, it is clear the policies FISMA set forth were insufficient in stopping the leak.

Another, more recent example is the SolarWinds data breach (timeline shown in Fig. 4). In short, malicious actors accessed SolarWinds' system, inserting code into a seemingly secure regular update to a network monitoring software published by SolarWinds. Approximately 18,000 customers downloaded and installed this code, opening a backdoor to the monitoring software and, thus, the entire network. A few notable U.S. agencies affected by this hack included the Treasury, Justice, Defense, and Energy Departments [28].

This breach is especially concerning because it went undetected for months in agencies that effectively implemented FISMA policies and NIST/DHS standards. CISA, the

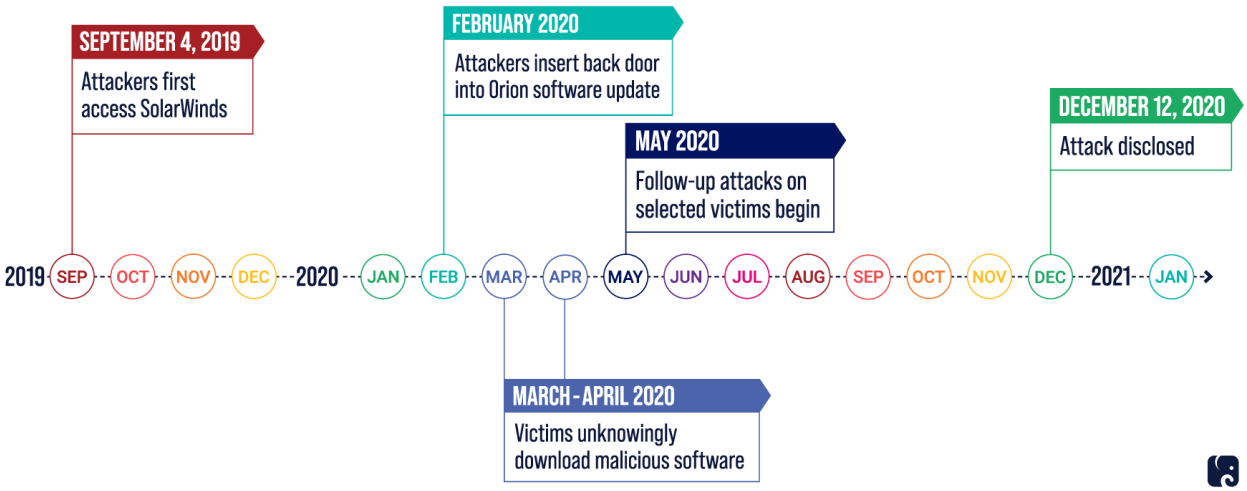

Figure 4. SolarWinds breach timeline [55].

agency tasked with many cybersecurity software suites for the U.S. government, was also compromised by the SolarWinds breach. The detection systems used by CISA and other agencies primarily depends on known attacks and finding matching code in internet systems, not new attacks like SolarWinds in trusted software. Once the attackers installed and activated their backdoor, near uninterrupted network access was provided to them.

The Colonial Pipeline breach is another example of a recent cyberattack. Thought to originate from a bad network configuration, the company responsible for 45 percent of the gas and jet fuel delivery on the United States' East Coast suffered a ransomware attack early May 2021 [29]. The pipeline company ultimately paid a cryptocurrency ransom of over $4 million. Even a month after the attack, the IT infrastructure was not fully restored.

In a May 2021 Senate Armed Services cyber subcommittee hearing, Pentagon officials were questioned on how to prevent another infrastructure ransomware attack. Witnesses testified that the hack was not required to be reported to the Pentagon, DHS, or other agency. This lack of notification was not exclusive to the Colonial Pipeline breach; SolarWinds also did not provide notice to affected customers.

The final example is the September 2017 Equifax data breach in which the personal information – amounting to terabytes of data – of 147 million people was exposed [30]. With an unknown long-term cost and a $425 million settlement, this breach may be the worst in the last five years. From a known but unpatched vulnerability in Equifax's web portal, attackers were able to enter their network and move between servers freely due to a lack of network segmentation. Equifax did not publicize the breach until more than a month after they detected the intrusion, like the SolarWinds and Colonial Pipelines breaches.

From the described examples of significant data breaches inside U.S. government agencies, in government contractors, and corporations affecting millions of U.S.

citizens, it is clear that human error has significant cost. Due to the lack of network segmentation, the lack of FISMA compliance, and ultimately taking an outdated approach to network security, multiple IT systems were breached in significant and long-lasting ways.

2.4 Economic impact of action

The cost of both action and inaction are considerable. The goal, of course, is to minimize the cost of action relative to inaction with the hope of no network security breaches. The general tradeoff of action and inaction is discussed in this section.

As stated previously in the 2020 IBM security report, the U.S. suffered an average cost per data breach of $8.64 million over the hundreds of tracked breaches with an expected increase over the next years. Eighty percent of these breaches contained customer personally identifiable information which is likely to further increase the price per breach for every subsequent year.

This IBM report did not directly factor in mega-breaches like Equifax or SolarWinds (in the respective years reports) which have costs in the hundreds of millions of dollars. Many consider these costs too high and demand action. These calls have not gone unnoticed, with Equifax investing over one billion dollars to improve their cybersecurity infrastructure. Whether to help restore customer's trust in the company or for a genuine concern for future breaches, the cost of action by Equifax proved substantial.

However large the cost of action, the cost of inaction will always be greater. An increasing number of local governments and municipalities are updating their infrastructure to modern systems. As opposed to primarily analog controls and functions, infrastructure is moving to digital connected devices. From the electric grid to water supply, digital controls are becoming more common.

With this move comes risks. If IT control and security systems do not change with modern infrastructure systems, significant vulnerabilities will be present at the most fundamental levels. Not acting to improve these systems will incur too high of a price if the water supply, electricity grid, or other services are compromised. Investing in sensible and effective cybersecurity technologies and training are necessary to mitigate and eliminate fallout from inaction.

3. Recommendations

Both the U.S. government – including its contractors and subcontractors – and the private sector must improve their information technology infrastructure by implementing zero trust systems and zero trust architecture to mitigate risks from current and future cybersecurity threats. Current systems too frequently contain outdated assumptions and system configurations for modern attacks, and the prevalence of human error is too significant to not be contained. The remainder of this section will detail specific recommendations, paths for implementation, and costs associated with each path.

3.1 Improved FISMA enforcement

The OMB should allocate additional funding for CISA, specifically in their auditing services. With effective audits, agencies can detect and mitigate vulnerabilities in their IT infrastructure. Even after nearly two decades of FISMA, many U.S. departments and agencies are not completely FISMA compliant. The noncompliance issues as discussed are not exclusive to the OPM and VA. IG reports from many agencies have shown, on average, an increasing degree of compliance and stronger networks on average, but this is not sufficient.

3.1.1 Objectives and impact

While the goal for IT systems and networks is to become more in-line with FISMA directives and NIST standards, more specific objectives are necessary. Agencies must closely consider broad scale cybersecurity without necessarily implementing the bare minimum to satisfy requirements. With the proposed recommendations, a shift in mindset for agency security is encouraged for continued success in system management.

Without undercutting necessary cybersecurity funding, consequences to encourage FISMA compliance are necessary. For these entities to effectively implement strong cybersecurity networks, funding for IT systems is required. Removing funding year after year for non-compliance contributes to a positive feedback loop harmful to both the agency and the government as a whole. The OMB should help agencies and other entities with compliance rather than punish non-compliant groups.

An additional key objective for improved FISMA enforcement is better auditing by DHS and more specifically CISA. Currently tasked with assisting other agencies in their cybersecurity systems, CISA analyzes the network security of a requested agency at a particular point in time (as opposed to tracking network performance). These audits should be timelier and more effective for all IT systems.

The impacts of improving FISMA enforcement will be immediate and significant. Perhaps the most significant is stronger cybersecurity systems. With many agencies still lacking in implementing FISMA requirements, it is clear that with better enforcement the minimum standards will be met, and a better national IT infrastructure will result.

3.1.2 Implementation

Due to a combination of insufficient staffing and growing cybersecurity networks, the request for audits cannot meet the current capacity to perform these audits. This mismatch is causing an increasing backlog of audit requests. Especially as more devices and users are connected or added to federal systems and networks, the complexity of any given audit has risen accordingly. The main way to know what to improve in an IT system is knowing what is broken – which is addressed through these audits.

Through an addition to an allocations bill, increased funding should be given to both DHS as a whole and CISA in particular to conduct cybersecurity audits and provide recommendations to agencies on system improvements. The exact allocations may need an independent investigation to determine how many more staff and resources are required to match or exceed demand. The current FY2022 Homeland Security funding bill has allocated $2.42 billion for CISA, broken into multiple categories [43]. For "mission support activities," which includes auditing, only three million dollars have been allocated.

The Homeland Security subcommittee should revise their proposed budget and increase allocations for mission support activities and more specifically their auditing program. At least an additional $2 million should be allocated for effective auditing in the support of FISMA enforcement.

As briefly described in this document's appendix, BOD 19-02 requires agencies to review and mitigate vulnerabilities found by DHS within 30 days of notification. The current development of technology, software, and security too frequently outpaces the auditing and mitigation timeline. With an increase in the abilities of CISA through greater allocations, federal agencies can manage FISMA requirements and IT system cybersecurity.

Figure 5. CISA audit request [56].

3.2 Revise NIST Special Publication 800-207

NIST SP 800-207 was written with the purpose of defining ZT and ZTA along with providing general deployment models and use cases. While providing a definition with a few examples is a good start, this guidance does not go far enough in detail in a few key areas. These areas include legacy system information, deployment cases, and responsibilities.

3.2.1 Objectives and impact

It is commonly known that the U.S. government operates a wide variety of legacy systems, from the federal to municipal level. Whether outdated software or hardware, thousands of these older systems are in use. Implementation of ZT systems is much easier when built from the ground up. Analogous to smart cities where many devices communicate between each other in a wide connected network, converting outdated infrastructure to modern technology is harder than integrating smart systems into new development. This applies to legacy systems as well.

SP 800-207 should better address integration examples, procedures, and implementations for legacy systems across federal and state entities in their transition to modern cybersecurity practices and ZTA. This publication should include specific guidelines for a variety of legacy systems in their move to ZTA. Although not all legacy systems can directly integrate into a ZT system, additional protections can be included to more closely resemble ZTA. Including specific implementations and procedures for legacy systems will help local governments and federal agencies more quickly and effectively adopt ZT systems and policies.

An additional revision important to consider is improving the descriptions of the given use cases or deployment cases. This publication gives an overview of the network model rather than guidelines for implementation. In future revisions to SP 800-207, use cases should be more general with clear methods for implementation in each case. By including the suggested revisions, agencies and enterprises can save time and money when moving to a ZTA.

Finally, revisions to this publication should more clearly detail the individual or individuals responsible for implementation of ZT systems and ZTA along with giving them the influence necessary for implementation. FITARA expanded the reach of CIOs in an agency's IT systems for more centralized and clearer IT monitoring and policy. SP 800-207 acknowledges the Federal CIO Council yet does not give mention of responsibility in the document.

By meeting these objectives in subsequent revisions of SP 800-207, more useful and applicable information can be given to U.S. government entities in their move to the next generation of cybersecurity policy. With ZT systems becoming more prevalent, possible large-scale breaches can be effectively contained and stopped. Insider threats, unimpeded network access, and more will become insignificant issues in a ZTA system.

3.2.2 Implementation

More detailed deployment guidelines would considerably help agencies in implementing ZTA for their systems. SP 800-207 gives five deployment scenarios for enterprise environments with only a few paragraphs of description dedicated to each scenario, and little to no mention of legacy systems. The Information Technology Laboratory (ITL) at NIST should include a new section on legacy system integration, expand the use case examples, and include more detail to help implement the use cases.

As legacy systems are difficult to define due to their large variety, overarching integrations need to be addressed. Specific firewall and router configurations, detailed network segmentation procedures, and even isolation techniques should be written into the revision. Not all legacy systems can directly integrate securely with modern technology, so the operation of multiple or isolated networks would not be uncommon.

The given use cases in SP 800-207 are both too narrow and not specific enough. ZT systems should not be limited to a set number of cases. ZTA looks to replace outdated models of perimeter-based network security, so it makes the most sense for every system to implement a ZT model. Changing the phrasing and general tone of this publication from an overview of ZT systems to be more inclusive of every IT system will help government entities in their ZTA approach.

Revision of this publication should describe who is responsible for ZTA implementation and subsequent monitoring associated with good ZTA policy. EO 10460 attempts to patch the lack of stated responsibility by requiring the head of each agency to develop a plan for implement ZTA within sixty days of the date of the order (middle of July) [11]. However effective this order is, NIST should revise its publication to assign responsibility for ZTA implementation.

A future administration is unlikely to prioritize removing policies in EO 10460. However, including specifics from NIST congregates and solidifies responsibilities. To implement the revisions discussed, a thorough processes is needed by NIST and specifically its ITL. The ITL is responsible for the 800 series of publications and ultimately SP 800-207. The current director of the ITL, Charles Romine, should be notified of proposed revisions for further discussion.

3.3 Allocate funding for IT services and small businesses

Better cybersecurity systems require better funding. Across the U.S. government, IT services are underfunded and understaffed. This is clear from the lack of FISMA compliance along with analyzing budget allocations. Additionally, hundreds of government sub-contractors are small businesses that lack the support of large IT departments and thus have generally weaker cybersecurity systems. As of 2015, as much as 43 percent of cyberattacks target small business, with an increasing upwards trend following [32]. Small businesses also account for thousands of subcontractors, with one large aircraft manufacturer working with 12,000 small businesses [33]. Through the OMB or Congress, funding should be allocated to U.S. government IT services and programs to support the IT services of small business.

From software to personnel, significant appropriations are needed to operate IT systems to their best capacity, especially with ZT systems. A key part of ZTA is sensors to monitor network traffic at multiple points and in multiple network layers. To efficiently mitigate threats and maintain usual network use, software suites are used to monitor and respond to sensor data faster than a standard IT professional. Installing,

configuring, and analyzing data from these sensors is expensive, but an expense worthwhile for maintaining effective security systems.

3.3.1 Objectives and impact

The primary goal of targeting IT services and small businesses is to help provide support commonly found in large and well-funded IT departments to agencies and businesses without the capability for current significant investment. Especially with the increasing prevalence of ZT systems, more resources are needed to monitor and respond to threats.

By allocating more funding in these areas, IT services from the federal to municipal level have a significantly higher ability to adequately respond to cybersecurity threats and network monitoring. Through more staffing and better software resources, smaller departments can handle larger threats.

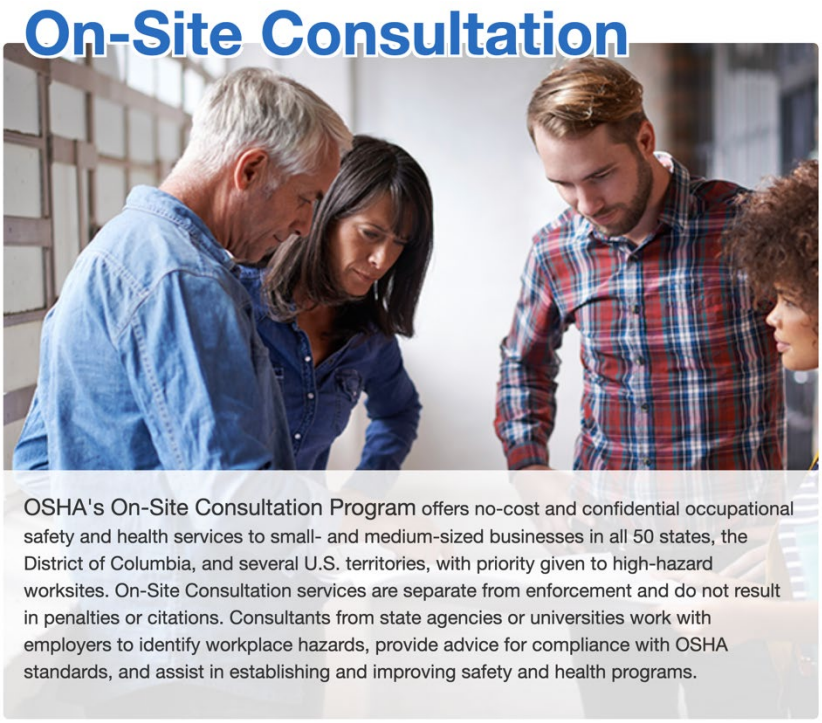

Figure 6. OSHA consultation program [48].

A key objective is also vulnerability recognition and mitigation. With a wide variety of cybersecurity threats and points of attack, the likelihood of a small IT department recognizing and closing all holes in their network is minimal. Having a U.S. agency be able to help small businesses identify and protect against system vulnerabilities will significantly impact and improve cybersecurity in America.

3.3.2 Implementation

Taking a methodology from the Occupational Safety and Health Administration (OSHA), an investment in consultation services for cybersecurity systems offered by CISA should occur. OSHA partners with private companies to inspect businesses and provide recommendations for OSHA compliance. For small businesses, this service is of no cost provided they implement all recommendations. Transferring the same concept to CISA allows for an increase in secure IT systems for small businesses without incurring significant costs by the small business.

Either with increased allocations from Congress or by using a portion of the current CISA budget, programs for small business cybersecurity network consulting should be implemented following a similar model to OSHA. The initial focus should be with

contractors and subcontractors on ZTA, with an expansion to more entities and overall network infrastructure after a successful rollout.

Strengthening the IT foundations of U.S. entities will have direct and significant benefits for cybersecurity. Less successful attacks, less severe breaches, and a culture shift will all result from increased allocations to IT services and consulting.

3.4 Require mandatory reporting

The U.S. government does not currently mandate reporting of cybersecurity breaches and data leaks for corporations. The Equifax and SolarWinds data breaches, which affected thousands of government employees and millions of others, were not initially disclosed to the DHS, NSA, or other federal entity. When looking at OSHA policies, they require reporting of workplace deaths, hospitalizations, and more to help ensure worker and workplace safety. Similar requirements must be implemented for cybersecurity attacks.

The path to implementation may be easiest via DHS's Binding Operational Directives (BODs). Issuing a new BOD is not trivial yet can be completed in a timely manner. Especially when considering the importance and simplicity of the directive, there is no reason for a non-expedited process. Two key points in the proposed BOD are the requirements for reporting and where to report. Companies reporting every successful and unsuccessful cyber-attack may be counterproductive, and the definition of a cyber-attack is vague. However, making the requirements for reporting more restrictive may allow companies to delay notification of a threat. Significant and novel data breaches and cybersecurity attacks should thus be reported.

Current policies and proposed legislation may also have an answer. The Transportation and Security Administration has mandated a 12-hour reporting window for critical pipeline infrastructure breaches in response to the Colonial Pipeline attack. A recent bill by Sens. Mark Warner (D-VA), Marco Rubio (R-FL), and Susan Collins (R-ME) requires federal agencies, contractors, and critical infrastructure companies to report successful cyberattacks to CISA within 24 hours and continue sharing novel information within 72 hours of discovery [44][45].

The bipartisan support of this bill is promising. This legislation should be passed with haste and enforced as soon as possible. Under this bill, CISA would be the receiving and processing agency. Since CISA already gives feedback to federal IT systems, they would most effectively be able to include data breach reporting in their services. Creating a hotline and online report page are initial steps and a public relations push should be addressed second. By mandating reporting, cybersecurity threats can more easily be identified and mitigated across the entire U.S. IT infrastructure from the local to federal level.

Final Notes

Since the start of network systems, a fight between keeping a system secure and hackers trying to breach it has existed. With an exponential rise in digital technology over the past two decades, a similar rise occurred with threats to network integrity. Through human error, malicious actors, and numerous vulnerabilities, thousands of data breaches have occurred and will continue to occur. It is up to everyone to create a culture shift in cybersecurity and revise outdated assumptions about networks. Through effective zero trust policy and zero trust systems, countless threats can be mitigated and stopped before they even start. Using the recommendations presented in this paper, the U.S. government can take the initial steps in further securing its IT infrastructure and making its citizens safer against cyberattacks.

Appendix

Important NIST Publications and DHS Binding Operational Directives

SP 800-53: *Security and Privacy Controls for Information Systems and Organizations* provides a catalog of security and privacy controls for information systems and organizations to protect organizational operations and assets, individuals, other organizations, and the Nation from a diverse set of threats and risks, including hostile attacks, human errors, natural disasters, structural failures, foreign intelligence entities, and privacy risks [10].

SP 800-207: *Zero Trust Architecture* contains an abstract definition of zero trust architecture and gives general deployment models and use cases where zero trust could improve an enterprise's overall information technology security posture [20]. This 2020 document helps agencies understand ZTA and ways to modify their systems.

SP 800-37: *Risk Management Framework for Information Systems and Organizations* describes the Risk Management Framework (RMF) and provides guidelines for applying the RMF to information systems and organizations. The RMF provides a disciplined, structured, and flexible process for managing security and privacy risk that includes information security categorization; control selection, implementation, and assessment; system and common control authorizations; and continuous monitoring [21].

SP 800-60: *Guide for Mapping Types of Information and Information Systems to Security Categories* has been developed to assist Federal government agencies to categorize information and information systems. The guideline's objective is to facilitate application of appropriate levels of information security according to a range of levels of impact or consequences that might result from the unauthorized disclosure, modification, or use of the information or information system [22].

FIPS Publication 199: *Standards for Security Categorization of Federal Information and Information Systems* defines the standard federal agencies must follow to assess the agency's information and IT systems for future appropriate security measures to be defined [17]. This document is the foundation for many subsequent standards by NIST or the DHS.

FIPS Publication 200: *Minimum Security Requirements for Federal Information and Information Systems* specifies minimum security requirements for information and information systems supporting the executive agencies of the federal government and a risk-based process for selecting the security controls necessary to satisfy the minimum security requirements [18].

BOD 18-02: *Securing High Value Assets* requires agencies to identify and report their high value IT assets to DHS along with allowing DHS to assess the security of and mitigate any vulnerabilities in the reported assets [23]. This BOD is helpful for both the agency in better defining their information system and DHS in increasing the security of federal systems.

BOD 19-02: ***Vulnerability Remediation Requirements for Internet-Accessible Systems*** requires agencies to review and mitigate vulnerabilities found by DHS within 30 days of notification [24]. This BOD encourages continuous weakness or vulnerability analysis in federal systems and a mitigation plan of possible threats.

BOD 20-01: ***Develop and Publish a Vulnerability Disclosure Policy*** requires agencies to create and publish policies on how the public can identify vulnerabilities in federal IT systems and alert the agency of a potential risk [25].

The preceding list of NIST standards and DHS publications is not intended to be comprehensive. However, these documents give federal agencies a clear path for IT system design, implementation, and vulnerability mitigation.

References

[1] "Timeline of Computer History: Memory and Storage." Accessed: Jun. 17, 2021. [Online]. Available: https://www.computerhistory.org/timeline/memory-storage/

[2] "How much data does google handle?" Accessed: Jun. 17, 2021. [Online]. Available: https://www.heshmore.com/how-much-data-does-google-handle/

[3] IBM Security, "Cost of a Data Breach Report 2020," IBM, 2020. [Online]. Available: https://www.ibm.com/security/digital-assets/cost-data-breach-report/

[4] "Psychology of Human Error," Tessian, Stanford. [Online]. Available: https://www.tessian.com/research/the-psychology-of-human-error/

[5] V. Zwass, "Information System," *Encyclopedia Britannica*, Nov. 03, 2020. https://www.britannica.com/topic/information-system (accessed Jun. 23, 2021).

[6] "Regulation (EU) 2016/679 of the European Parliament and of the Council." Apr. 16, 2016. [Online]. Available: http://data.europa.eu/eli/reg/2016/679/oj

[7] W. Ware, "Security Controls for Computer Systems: Report of the Defense Science Board Task Force on Computer Security." The Rand Corporation for the Office of the Director of Defense Research and Engineering. [Online]. Available: https://nsarchive.gwu.edu/document/21583-document-01-defense-science-board-task-force

[8] 44 U.S.C. §§3551-3559, *Federal Information Security Modernization Act.* 2014. [Online]. Available: https://www.congress.gov/bill/113th-congress/senate-bill/2521/text

[9] 40 U.S.C. §§11302, 11315, and 11319; and 44 U.S.C. §§3601, *Federal Information Technology Acquisition Reform Act*. 2014. [Online]. Available: https://www.congress.gov/bill/113th-congress/house-bill/1232

[10] Joint Task Force Interagency Working Group, "Security and Privacy Controls for Information Systems and Organizations," National Institute of Standards and Technology, Sep. 2020. doi: 10.6028/NIST.SP.800-53r5.

[11] The President, "Executive Order 14028 of May 12, 2021: Improving the Nation's Cybersecurity." Federal Register, May 12, 2021. [Online]. Available: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

[12] "Deciphering Executive Order 14028: Improving the Nation's Cybersecurity," *IIoT World*, May 28, 2021. https://iiot-world.com/ics-security/cybersecurity/deciphering-executive-order-14028-improving-the-nations-cybersecurity/

[13] C. Jaikaran, *Statement of Chris Jaikaran Analyst in Cybersecurity Policy Before Committee on Veterans' Affairs Subcommittee on Technology Modernization U.S. House of Representatives Hearing on "Cybersecurity and Risk Management at VA: Addressing Ongoing Challenges and Moving Forward."* 2021. [Online]. Available: https://crsreports.congress.gov/product/pdf/TE/TE10063

[14] "About CISA," *CISA*, 2021. https://www.cisa.gov/about-cisa

[15] D. Carr, "Building a protective black core for the Global Information Grid: An encrypted core would protect and segregate network traffic," *Defense Systems*, Sep. 09, 2009. https://defensesystems.com/articles/2009/09/02/cyber-defense-black-core.aspx (accessed Jun. 25, 2021).

[16] Office of Management and Budget, "Managing Information as a Strategic Resource," Washington, DC, Circular A-130, 2016. Accessed: Jun. 14, 2021. [Online]. Available: https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A130/a130revised.pdf

[17] National Institute of Standards and Technology, “Standards for security categorization of federal information and information systems,” National Institute of Standards and Technology, Gaithersburg, MD, NIST FIPS 199, Feb. 2004. doi: 10.6028/NIST.FIPS.199.

[18] National Institute of Standards and Technology, “Minimum security requirements for federal information and information systems,” National Institute of Standards and Technology, Gaithersburg, MD, NIST FIPS 200, Mar. 2006. doi: 10.6028/NIST.FIPS.200.

[19] VA IG, “Department of Veterans Affairs Federal Information Security Modernization Act Audit for Fiscal Year 2020,” Department of Veterans Affairs, Washington, DC, Audit 20-01927–104, Apr. 2021. [Online]. Available: https://www.va.gov/oig/pubs/VAOIG-20-01927-104.pdf

[20] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, “Zero Trust Architecture,” National Institute of Standards and Technology, Aug. 2020. doi: 10.6028/NIST.SP.800-207.

[21] Joint Task Force Interagency Working Group, “Risk Management Framework for Information Systems and Organizations,” National Institute of Standards and Technology, Dec. 2018. doi: 10.6028/NIST.SP.800-37r2.

[22] K. Stine, R. Kissel, W. Barker, J. Fahlsing, and J. Gulick, “Guide for Mapping Types of Information and Information Systems to Security Categories,” National Institute of Standards and Technology, Aug. 2008. doi: 10.6028/NIST.SP.800-60.

[23] “Binding Operational Directive 18-02: Securing High Value Assets.” U.S. Department of Homeland Security, May 07, 2018. [Online]. Available: https://cyber.dhs.gov/bod/18-02/

[24] “Binding Operational Directive 19-02: Vulnerability Remediation Requirements for Internet-Accessible Systems.” U.S. Department of Homeland Security, Apr. 29, 2019. [Online]. Available: https://cyber.dhs.gov/bod/19-02/

[25] “Binding Operational Directive 20-01: Develop and Publish a Vulnerability Disclosure Policy.” U.S. Department of Homeland Security, Sep. 02, 2020. [Online]. Available: https://cyber.dhs.gov/bod/20-01/

[26] Office of the Inspector General, “U.S. Office of Personnel Management Federal Information Security Modernization Act Audit for Fiscal Year 2020,” U.S. Office of Personnel Management, Washington, DC, Audit 4A-CI-00-20–010, Oct. 2020. [Online]. Available: https://www.opm.gov/our-inspector-general/publications/reports/2020/4a-ci-00-20-010.pdf

[27] “Cybersecurity Resource Center: CYBERSECURITY INCIDENTS,” *OPM.GOV*, 2015. https://www.opm.gov/cybersecurity/cybersecurity-incidents/

[28] D. Temple-Raston, “A ‘Worst Nightmare’ Cyberattack: The Untold Story of The SolarWinds Hack,” Apr. 16, 2021. https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack (accessed Jun. 27, 2021).

[29] S. Neuman, “What We Know About the Ransomware Attack on A Critical U.S. Pipeline,” May 10, 2021. https://www.npr.org/2021/05/10/995405459/what-we-know-about-the-ransomware-attack-on-a-critical-u-s-pipeline (accessed Jun. 27, 2021)

[30] J. Fruhlinger, “Equifax data breach FAQ: What happened, who was affected, what was the impact?,” *CSO*, Feb. 12, 2020. https://www.csoonline.com/article/3444488/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html (accessed Jun. 27, 2021).

[31] T. Riley, “Senate fails to confirm new CISA director before two-week break, drawing criticism,” Jun. 24, 2021. https://www.cyberscoop.com/cisa-senate-jen-easterly-confirmation/ (accessed Jun. 29, 2021).

[32] “Attackers Target Both Large and Small Businesses.” Broadcom, 2015. [Online]. Available: https://docs.broadcom.com/doc/istr-attackers-strike-large-business-en

[33] J. Grady, "Lawmakers Grill Pentagon Officials on How to Prevent Another Colonial Pipeline-Style Attack," *USNI News*, May 18, 2021. https://news.usni.org/2021/05/18/lawmakers-grill-pentagon-homeland-security-officials-on-how-to-prevent-another-colonial-pipeline-style-attack (accessed Jun. 28, 2021).

[34] F25 Committee, "Guide for Cybersecurity and Cyberattack Mitigation," ASTM International. doi: 10.1520/F3286-17.

[35] J. Hash, N. Bartol, H. Rollins, W. Robinson, J. Abeles, and S. Batdorff, "Integrating IT Security into the Capital Planning and Investment Control Process," National Institute of Standards and Technology, Jan. 2005. doi: 10.6028/NIST.SP.800-207.

[36] The Jericho Forum, "Jericho Forum Commandments." 2007. [Online]. Available: https://collaboration.opengroup.org/jericho/commandments_v1.2.pdf

[37] C. Cunningham, "Next-Generation Access and Zero Trust," *Forrester*, Mar. 27, 2018. https://go.forrester.com/blogs/next-generation-access-and-zero-trust/ (accessed Jun. 25, 2021).

[38] IATAC, "Defining the GIG Core." Summer 2008. [Online]. Available: https://www.csiac.org/wp-content/uploads/2016/02/Vol11_No2.pdf

[39] L. Pope, "What Is FISMA Compliance and Who Does It Impact?," Jun. 19, 2019. https://www.g2.com/articles/fisma-compliance (accessed Jun. 22, 2021).

[40] "OVERVIEW OF THE PRIVACY ACT OF 1974 (2020 EDITION)." U.S. Department of Justice, 2020. [Online]. Available: https://www.justice.gov/opcl/overview-privacy-act-1974-2020-edition

[41] 5 U.S.C. §§552a, *Privacy Act of 1974*, [Online]. Available: https://www.justice.gov/opcl/privacy-act-1974

[42] J. Hasg, N. Bartol, H. Rollins, W. Robinson, J. Abeles, and S. Batdorff, "Integrating IT Security into the Capital Planning and Investment Control Process," National Institute of Standards and Technology, Jan. 2005. doi: 10.6028/NIST.SP.800-65.

[43] "24. CYBERSECURITY FUNDING." U.S. Government Information, 2020. [Online]. Available: https://www.govinfo.gov/content/pkg/BUDGET-2020-PER/pdf/BUDGET-2020-PER-5-8.pdf

[44] "OSHA Reporting," *OSHA*. https://www.osha.gov/report

[45] Wolff, Josephine. "How Quickly Should Companies Have to Disclose Data Breaches?" Slate, June 24, 2021. https://slate.com/technology/2021/06/data-breach-disclosure-law-warner-rubio-collins.html.

[46] Geller, Eric, and Martin Matishak. "Senate Bill to Require Hack Reports within 24 Hours and Punish Violators." Politico, June 17, 2021. https://www.politico.com/news/2021/06/17/senate-bill-to-require-hack-reports-within-24-hours-and-punish-violators-495060.

[47] Kerman, Alper. "Zero Trust Cybersecurity: 'Never Trust, Always Verify.'" *NIST: Taking Measure* (blog), October 28, 2020. https://www.nist.gov/blogs/taking-measure/zero-trust-cybersecurity-never-trust-always-verify.

[48] OSHA. "OSHA Consultation," 2021. https://www.osha.gov/consultation.

[49] IEEE. "IEEE About," 2021. https://www.ieee.org/about/.

[50] WISE. "WISE About," 2021. https://wise-intern.org/home/the-program/about/.

[51] Office of the Inspector General. "U.S. Office of Personnel Management Federal Information Security Modernization Act Audit for Fiscal Year 2015." Audit. Washington, DC: U.S. Office of Personnel Management, November 10, 2015. https://www.opm.gov/our-inspector-general/publications/reports/2015/federal-information-security-modernization-act-audit-fy-2015-final-audit-report-4a-ci-00-15-011.pdf.

[52] Fruhlinger, Josh. “The OPM Hack Explained: Bad Security Practices Meet China’s Captain America.” CSO, February 12, 2020. https://www.csoonline.com/article/3318238/the-opm-hack-explained-bad-security-practices-meet-chinas-captain-america.html.

[53] Koerner, Brendan. “Inside the Cyberattack That Shocked the US Government.” Wired, October 23, 2016. https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/.

[54] Our World in Data. “Moore’s Law,” 2021. https://ourworldindata.org/grapher/transistors-per-microprocessor.

[55] Senate RPC. “THE SOLARWINDS CYBERATTACK,” January 29, 2021. https://www.rpc.senate.gov/policy-papers/the-solarwinds-cyberattack.

[56] CISA. “CISA Cyber Hygiene Services,” 2021. https://www.cisa.gov/cyber-hygiene-services.

[57] Curran, John. “White House Cyber EO Points Federal Agencies to Cloud, Zero Trust.” MeriTalk, May 13, 2021. https://www.meritalk.com/articles/white-house-cyber-eo-points-federal-agencies-to-cloud-zero-trust/.

[58] Field, Tom. “John Kindervag: Reflections on ‘Zero Trust,’” March 18, 2021. https://www.bankinfosecurity.com/john-kindervag-reflections-on-zero-trust-a-16209.

[59] Goodin, Dan. “NSA-Leaking Shadow Brokers Just Dumped Its Most Damaging Release Yet.” ARS Technica, April 14, 2017. https://arstechnica.com/information-technology/2017/04/nsa-leaking-shadow-brokers-just-dumped-its-most-damaging-release-yet/.

[60] Kelly, Mary Louise, Jason Fuller, and Justine Kenin. “The Colonial Pipeline CEO Explains The Decision To Pay Hackers A $4.4 Million Ransom.” NPR, June 3, 2021. https://www.npr.org/2021/06/03/1003020300/colonial-pipeline-ceo-explains-the-decision-to-pay-hackers-4-4-million-ransom.

[61] Perlroth, Nicole, and Scott Shane. “In Baltimore and Beyond, a Stolen N.S.A. Tool Wreaks Havoc.” The New York Times, May 25, 2019. https://www.nytimes.com/2019/05/25/us/nsa-hacking-tool-baltimore.html.

[62] RSI Security. “PENALTIES FOR NON-COMPLIANCE WITH FISMA (AND HOW TO AVOID THEM).” RSI, December 20, 2018. https://blog.rsisecurity.com/penalties-for-non-compliance-with-fisma-and-how-to-avoid-them/.

[63] Smith, Jordan. “Fed Officials Thankful for Cyber EO in Advancing Zero Trust Architecture.” MeriTalk, June 17, 2021. https://www.meritalk.com/articles/fed-officials-thankful-for-cyber-eo-in-advancing-zero-trust-architecture/.

[64] Sobers, Rob. “134 Cybersecurity Statistics and Trends for 2021.” Varonis, March 16, 2021. https://www.varonis.com/blog/cybersecurity-statistics/.

[65] Federal Trade Commission. “Equifax Data Breach Settlement,” January 2020. https://www.ftc.gov/enforcement/cases-proceedings/refunds/equifax-data-breach-settlement.

[66] Palo Alto Networks. “What Is a Zero Trust Architecture,” 2021. https://www.paloaltonetworks.com/cyberpedia/what-is-a-zero-trust-architecture.

[67] CyberArk. “The Principle of Least Privilege.” Accessed June 18, 2021. https://www.cyberark.com/what-is/least-privilege/.