DESIGN VS. DEFAULT: ANALYZING SHIFTS IN CYBERSECURITY

HEARING

BEFORE THE

SUBCOMMITTEE ON CYBERSECURITY AND INFRASTRUCTURE PROTECTION

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED EIGHTEENTH CONGRESS

SECOND SESSION

DECEMBER 5, 2024

Serial No. 118–84

Printed for the use of the Committee on Homeland Security

Available via the World Wide Web: http://www.govinfo.gov

U.S. GOVERNMENT PUBLISHING OFFICE
60–205 PDF WASHINGTON : 2025

COMMITTEE ON HOMELAND SECURITY

Mark E. Green, MD, Tennessee, *Chairman*

Michael T. McCaul, Texas
Clay Higgins, Louisiana
Michael Guest, Mississippi
Dan Bishop, North Carolina
Carlos A. Gimenez, Florida
August Pfluger, Texas
Andrew R. Garbarino, New York
Marjorie Taylor Greene, Georgia
Tony Gonzales, Texas
Nick LaLota, New York
Mike Ezell, Mississippi
Anthony D'Esposito, New York
Laurel M. Lee, Florida
Morgan Luttrell, Texas
Dale W. Strong, Alabama
Josh Brecheen, Oklahoma
Elijah Crane, Arizona

Bennie G. Thompson, Mississippi, *Ranking Member*
Eric Swalwell, California
J. Luis Correa, California
Troy A. Carter, Louisiana
Shri Thanedar, Michigan
Seth Magaziner, Rhode Island
Glenn Ivey, Maryland
Daniel S. Goldman, New York
Robert Garcia, California
Delia C. Ramirez, Illinois
Robert Menendez, New Jersey
Thomas R. Suozzi, New York
Timothy M. Kennedy, New York
LaMonica McIver, New Jersey
Yvette D. Clarke, New York

Stephen Siao, *Staff Director*
Hope Goins, *Minority Staff Director*
Sean Corcoran, *Chief Clerk*

SUBCOMMITTEE ON CYBERSECURITY AND INFRASTRUCTURE PROTECTION

Andrew R. Garbarino, New York, *Chairman*

Carlos A. Gimenez, Florida
Mike Ezell, Mississippi
Laurel M. Lee, Florida
Morgan Luttrell, Texas
Mark E. Green, MD, Tennessee *(ex officio)*

Eric Swalwell, California, *Ranking Member*
Troy A. Carter, Louisiana
Robert Menendez, New Jersey
LaMonica McIver, New Jersey
Bennie G. Thompson, Mississippi *(ex officio)*

Cara Mumford, *Subcommittee Staff Director*
Moira Bergin, *Minority Subcommittee Staff Director*

CONTENTS

Page

STATEMENTS

WITNESSES

APPENDIX

DESIGN VS. DEFAULT: ANALYZING SHIFTS IN CYBERSECURITY

Thursday, December 5, 2024

U.S. House of Representatives,
Committee on Homeland Security,
Subcommittee on Cybersecurity and
Infrastructure Protection,
Washington, DC.

The subcommittee met, pursuant to notice, at 10:05 a.m., in room 310, Cannon House Office Building, Hon. Andrew R. Garbarino (Chairman of the subcommittee) presiding.

Present: Representatives Garbarino, Ezell, Lee, Swalwell, Menendez, and McIver.

Mr. Garbarino. The Committee on Homeland Security Subcommittee on Cybersecurity and Infrastructure Protection will come to order.

Without objection, the Chair is authorized to declare the committee in recess at any point.

The purpose of this hearing is to receive testimony from a panel of industry leaders who will provide their perspectives on CISA's Secure by Design initiative, including Secure by Design pledge, which captures the initiative's principles.

I now recognize myself for an opening statement.

Good morning.

As cyber threats grow more advanced by the day, enhancing our cybersecurity posture has become one of the defining challenges of our time. This is due in part to how we have traditionally treated cybersecurity—as an add-on rather than essential.

We have relied on patches and software updates to fix vulnerabilities once they are discovered. Now that malicious actors can exploit weaknesses faster that we can address them, our reactive approach will not suffice.

To address this issue, CISA launched the Secure by Design initiative in April 2023, an effort that encourages companies to prioritize cybersecurity at the outset of product development.

As part of this initiative, CISA created a pledge that captures the 7 key pillars of what it means to be secure by design. These encompass actions from improving software security to increasing transparency about incidents.

Since the pledge was released in May, over 250 companies have signed on, underscoring wide-spread industry support and commitment to raising the bar for basic cybersecurity practices.

Today's hearing provides a valuable opportunity to dive deeper into the Secure by Design framework. In particular, we will consider how Secure by Design has benefited individual companies while enhancing cybersecurity across sectors and our Nation.

From my perspective, Secure by Design is a proactive commitment to making cybersecurity part of a company's core mission. It represents a shift toward viewing security and innovation as complementary, not competing, priorities.

As consumers, we must not only want but also expect that products we purchase are secure out of the box. To that end, we must remember that this initiative has worked because it has been voluntary. To continue to incentivize security as a standard practice rather than a costly add-on, it must continue to have industry buy-in.

Companies have implemented Secure by Design principles at a speed and scale that suits their business model. Likewise, CISA has fulfilled its role as a trusted partner by offering implementation guidance and facilitating critical conversations with pledge signatories.

I look forward to discussing the pledge's successes, challenges, and potential for the future. We risk losing the collaboration of companies that are forced to adopt requirements that they cannot meet, especially since many are already burdened with duplicative cyber regulations.

I want to thank our witnesses for their time and expertise. Your insights are critical as we work to strike a partnership between Government, industry, insurers, and other stakeholders in the cybersecurity ecosystem.

I hope this discussion about the Secure by Design initiative will provide a clear picture of what is working, where gaps remain, and how we can continue building the partnerships and policies necessary to enhance our Nation's cybersecurity posture.

Thank you, and I look forward to our conversation.

[The statement of Chairman Garbarino follows:]

Statement of Chairman Andrew R. Garbarino

December 5, 2024

Good morning.

As cyber threats grow more advanced by the day, enhancing our cybersecurity posture has become one of the defining challenges of our time. This is due in part to how we have traditionally treated cybersecurity: as an add-on, rather than essential.

We have relied upon patches and software updates to fix vulnerabilities once they are discovered. Now that malicious actors can exploit weaknesses faster than we can address them, our reactive approach will not suffice.

To address this issue, CISA launched the "Secure by Design" initiative in April 2023—an effort that encourages companies to prioritize cybersecurity at the outset of product development.

As part of this initiative, CISA created a pledge that captures the 7 key pillars of what it means to be "Secure by Design." These encompass actions for improving software security, to increasing transparency about incidents.

Since the pledge was released in May, over 250 companies have signed on, underscoring wide-spread industry support and commitment to raising the bar for basic cybersecurity practices.

Today's hearing provides a valuable opportunity to dive deeper into the Secure by Design framework. In particular, we'll consider how Secure by Design has benefited individual companies while enhancing cybersecurity across sectors and our Nation.

From my perspective, Secure by Design is a proactive commitment to making cybersecurity part of a company's core mission. It represents a shift toward viewing security and innovation as complementary, not competing, priorities. As consumers, we must not only want, but also expect, that products we purchase are secure out of the box.

To that end, we must remember that this initiative has worked because it has been voluntary. To continue to incentivize security as a standard practice rather than a costly add-on, it must continue to have industry buy-in.

Companies have implemented Secure by Design principles at a speed and scale that suits their business model. Likewise, CISA has fulfilled its role as a trusted partner by offering implementation guidance and facilitating critical conversations with pledge signatories. I look forward to discussing the pledge's successes, challenges, and potential for the future.

We risk losing this collaboration if companies are forced to adopt requirements which they cannot meet—especially since many are already burdened with duplicative cyber regulations.

I want to thank our witnesses for their time and expertise. Your insights are critical as we work to strengthen partnerships between Government, industry, insurers, and other stakeholders in the cybersecurity ecosystem.

I hope this discussion about the Secure by Design initiative will provide a clearer picture of what's working, where gaps remain, and how we can continue building the partnerships and policies necessary to enhance our Nation's cybersecurity posture.

Thank you, and I look forward to our conversation.

Mr. GARBARINO. I now recognize the Ranking Member, the gentleman from California, Mr. Swalwell, for his opening statement.

Mr. SWALWELL. Good morning.

I would like to thank Chairman Garbarino for holding today's hearing on Secure by Design and secure by default.

In recent decades, we have witnessed remarkable technological progress that has changed every aspect of our lives. With rapid advances in AI, we can expect that transformation to continue in the years ahead.

Much of this innovation has taken place, of course, in America but also in my Congressional district. I am looking forward to hearing from Mr. Srinivas Mukkamala in particular, my invited guest, because of his connection to my district.

The competition between technology companies globally has also led to the development of new products and services that have benefited people around the world.

A challenge with this digital revolution is that the innovation that has transformed how we communicate, store our data, and access vital services has not always been matched with the level of security necessary to protect us from foreign adversaries and criminal gangs. Every day, we read about cyber incidents that demonstrate the security built into our digital ecosystem and that it is insufficient to protect our privacy or critical infrastructure.

To combat this problem, we must rely on the same innovative spirit that has fueled our recent technological progress to also transform our security. This idea underpinned President Biden's National Cybersecurity Strategy when it was committed to building toward a future digital ecosystem that is more inherently defensible and resilient.

Under Director Easterly's leadership, CISA has led the way with its Secure by Design initiative, partnering with allied countries and private-sector partners to develop principles on how we can better embed security into technology.

Critical is an understanding that security must primarily be the responsibility of those with the most resources and expertise. For too long, the response to many cyber incidents is a reminder to turn on multifactor authentication or training on how to spot a phishing attack.

Don't get me wrong; there is a role for cybersecurity training and best practices for end-users. But humans are fallible, and asking consumers to defend themselves against well-resourced criminal gangs and nation-state actors is a doomed strategy. Instead, we must reduce the burden on end-users by embedding security into technology and turning on security features by default.

I would also like to just acknowledge Ms. Adkins, who is representing Google. I have noticed in my own Gmail some of the recent upgrades that make it much harder for an outside actor to access Gmail, and I think all users are appreciative of that.

This fundamental shift in how we think about security will not be easy, and it will take time, resources, and cooperation between Government and the private sector. The efforts we have seen under the Biden administration have made significant progress, but we must continue this initiative in the coming years.

Today's hearing is an opportunity to hear directly from private-sector experts on the promise of Secure by Design, the challenges we will face in shifting to this new paradigm, and how the Federal Government can support and incentivize improved security.

It is critical that terms like "secure by design" and "secure by default" are not just buzzwords and marketing schemes but result in meaningful change. I hope our witnesses will help this subcommittee better understand how we can support private-sector innovations in security and move toward a more secure digital ecosystem.

Before I close, this is likely our last subcommittee hearing before a new administration takes place. CISA's Secure by Design initiative is just one example of the many vital projects that CISA carries out. Efforts in the next administration to weaken or abolish CISA could have devastating impacts on our national security, and I hope that we can continue to work, as we have this Congress under the Chairman's leadership, in a bipartisan way to support this vital agency.

With that, I look forward to the witnesses and their testimony. I yield back. Thank you.

[The statement of Ranking Member Swalwell follows:]

Statement of Ranking Member Eric Swalwell

December 5, 2024

In recent decades, we have witnessed remarkable technological progress that has changed every aspect of our lives, and with rapid advances in AI, we can expect this transformation to continue in the coming years.

Much of this innovation has taken place here in America, including in my district in the Bay Area, and the competition between technology companies globally to develop new products and services has benefited people around the world.

A challenge with this digital revolution is that the innovation that has transformed how we communicate, store our data, and access vital services has not always been matched with a level of security necessary to protect us from foreign adversaries and criminal gangs.

Every day we read about cyber incidents that demonstrate the security built into our digital ecosystem is insufficient to protect our privacy or critical infrastructure.

To combat this problem, we must rely on the same innovative spirit that has fueled our recent technological progress to also transform how we secure our networks.

This idea underpinned President Biden's National Cybersecurity Strategy when it committed to "building toward a future digital ecosystem that is more inherently defensible and resilient."

And under Director Easterly's leadership, CISA has led the way with its Secure by Design Initiative, partnering with allied countries and private-sector partners to develop principles on how we can better embed security into technology going forward.

Critical to this effort is an understanding that security must primarily be the responsibility of those with the most expertise and resources.

For too long, the response to many cyber incidents is a reminder to turn on multifactor authentication or training on how to spot a phishing attack.

Don't get me wrong—there's a role for cybersecurity training and best practices for end-users.

But, humans are fallible, and asking consumers to defend themselves against well-resourced criminal gangs and nation-state actors is a doomed strategy.

Instead, we must reduce the burden on end-users by embedding security into technology and turning on security features by default.

This fundamental shift in how we think about security will not be easy, and it will take time, resources, and cooperation between Government and the private sector.

The efforts we have seen under the Biden administration have made significant progress, but we must continue this initiative in the coming years.

Today's hearing will be an opportunity to hear directly from private-sector experts on the promise of Secure by Design, the challenges we will face in shifting to this new paradigm, and how the Federal Government can better support and incentivize improved security.

It is critical that terms like secure by design and secure by default not become buzzwords in marketing schemes but instead result in meaningfully improved security outcomes.

I hope our witnesses will help this subcommittee better understand how we can support private sector innovations in security and move toward a more secure digital ecosystem.

Before I close, this is likely our last subcommittee hearing before a new administration takes office.

CISA's Secure by Design Initiative is just one example of the many vital projects CISA carries out.

Efforts in the next administration to weaken or abolish CISA could have devastating impacts on our national security, and I hope we can work in a bipartisan way to support this vital agency.

Mr. GARBARINO. Thank you, Ranking Member Swalwell.

Other Members of the committee are reminded that opening statements may be submitted for the record.

[The statement of Ranking Member Thompson follows:]

STATEMENT OF RANKING MEMBER BENNIE G. THOMPSON

DECEMBER 5, 2024

When President Biden and Vice President Harris were sworn in 4 years ago, they committed to making cybersecurity a national security priority, and they have.

From the May 2021 Executive Order on Improving the Nation's Cybersecurity, to the March 2023 National Cybersecurity Strategy, to the July 2023 National Cyber Workforce and Education Strategy, the Biden-Harris administration has put in place ambitious policies to secure our digital ecosystem.

A common thread in these efforts has been identifying systemic approaches to improving security.

Notably, the National Cyber Strategy articulated a pivotal shift in responsibility for security—away from consumers and onto software developers and technology manufacturers who are better positioned to systemic action reduce cyber risk.

Too frequently, the technology we rely on every day is vulnerable to attack because manufacturers prioritized being first to market over being the most secure in the market.

As CISA Director Jen Easterly observed: "We don't have a cybersecurity problem. We have a software quality problem."

With that in mind, I commend CISA for launching the Secure by Design Initiative and encouraging software manufacturers to take the steps necessary to ensure their products are secure when their customers use them.

I am pleased that over 200 companies have signed CISA's Secure by Design Pledge, including some of our witnesses today.

I will be interested in understanding how witnesses have improved their development practices since signing the Pledge, and how CISA can incentivize and facilitate greater adoption of Secure by Design practices in the future.

At the same time, I recognize that the Secure by Design Initiative is a voluntary program with no enforcement mechanism.

We would be remiss if we did not explore the limitations of relying on voluntary programs to improve the security of technology that underpins our communications infrastructure, our health care infrastructure, Federal networks, and other critical infrastructure sectors.

Before I close, I will note that that this is the last cybersecurity hearing we will hold during the Biden-Harris administration.

Project 2025, which was written by people close to the President-elect, included a series of troubling, ill-informed proposals for CISA's future that would diminish its ability to effectively defend Federal networks and carry out its broad infrastructure security mission.

I hope my colleagues on this panel will educate the incoming administration about CISA's important missions and push back against efforts to undermine the agency in the weeks and months ahead.

Mr. GARBARINO. I am pleased to have a distinguished panel of witnesses before us today on this very important topic.

I ask that our witnesses please rise and raise their right hand.

[Witnesses sworn.]

Mr. GARBARINO. Let the record reflect that the witnesses have answered in the affirmative.

Thank you, and please be seated.

I would like to now formally introduce our witnesses.

Heather Adkins is a 22-year Google veteran and a founding member of the Google Security Team. As VP of security engineering and head of Google's Office of Cybersecurity Resilience, she has built a global team responsible for maintaining the safety and security of Google's networks, systems, and applications. She is co-author of the book "Building Secure & Reliable Systems" and has advised numerous organizations on how to adopt modern, defendable architectures.

Shane Fry is the CTO at RunSafe Security, Inc. He has over a decade of experience in cybersecurity, both offensive and defensive. Shane began his career performing vulnerability assessments on a variety of software platforms. His research has spanned all the layers of the hardware and software stack, including physical circuit security, secure boot, software updates, memory corruption, and web application vulnerabilities. Shane has worked for the U.S. Government, a large prime contractor, and numerous cybersecurity start-ups.

Mr. Jim Richberg is Fortinet's head of cyber policy and global field CISO. This role enables him to leverage his nearly 40 years' experience driving innovation in cybersecurity and threat intelligence. Prior to joining Fortinet, Jim served as the U.S. National Intelligence Manager for Cyber, the senior Federal executive focused on cyber intelligence within the U.S. intelligence community. He led the creation and implementation of the cyber strategy for the 17 departments and agencies of the IC, set integrated priorities on the cyber threat, and served as the senior advisor to the director of national intelligence on cyber issues.

Dr. Srinivas Mukkamala—is that right? Wonderful—serves on the Board of Regents for New Mexico Tech; independent board member of El Paso Electric; State of New Mexico's Governor's advisor on AI and cybersecurity; advisor to Cowbell Cyber and advisor to SecurityScorecard, among many other advisory roles.

How are you here today? That's a lot of work.

He served as chief product officer for Ivanti, where he was responsible for product management and engineering. Dr. Mukkamala founded RiskSense, a recognized leader in risk-based vulnerability management. Ivanti acquired RiskSense in 2021.

I thank all the witnesses for being here today.

I now recognize Ms. Adkins for 5 minutes to summarize her opening statement.

STATEMENT OF HEATHER ADKINS, VICE PRESIDENT, SECURITY ENGINEERING, GOOGLE

Ms. ADKINS. Thank you.

Chairman Garbarino, Ranking Member Swalwell, and other Members of the committee, thank you for the opportunity to speak here today. I am Heather Adkins, and I'm vice president of security engineering at Google.

Billions of people today rely on technology in their daily lives—to run their businesses, further their education, for entertainment, shopping, and many other things. In this interconnected world, it's critical that we ensure technology systems are resilient to keep people safe. As we know from the news, that is not always the case.

Throughout my career in cybersecurity, I've had a good vantage point from which to study how security breaches occur and the succession of events that cause them. What I've learned is that whether or not a system is resilient is a question of whether it's designed properly. Cybersecurity is an inherent property of the system, in the same way that safety is an inherent property of an automobile.

For this reason, for over 20 years, Google has pioneered a Secure by Design approach, long before we called it that, embedding security into every phase of the software development life cycle, not just the beginning or the end. This year, we published a detailed white paper on our approach, titled "An Overview of Google's Commitment to Secure by Design." My testimony today will share some insights from that paper.

First, we know that many attacks start with social engineering, where an attacker tricks a user into taking harmful action. In 2023 alone, Americans lost $12.5 billion to phishing and scams.

To combat these kinds of threats, Google has invested in bringing multifactor authentication to all of our users. This journey dates back to 2010, when we launched Google Authenticator and two-step verification for Google Workspace. Since then, we have expanded this to all of our services and worked with the FIDO Alliance, an industry coalition, to develop standardized hardware tokens to stop password phishing.

This coalition has also developed industry standards such as passkeys, a passwordless sign-in experience which has been used to authenticate users more than 1 billion times. The industry goal is to eliminate passwords altogether—a design flaw on the internet that has persisted for decades.

Second, attackers exploit entire classes of vulnerabilities that stem from how software is written. We've been working proactively to reduce the incidence of these as well.

Our approach starts with safe coding frameworks and secure development environments, meaning we give our developers the tools to write safe code by default rather than relying on them to understand everything about cybersecurity.

By doing this, we've been able to prevent many of MITRE's 25 most dangerous software weaknesses from entering our code base, such as cross-site scripting, the No. 1 weakness; SQL injection, the No. 3; and others. By reducing the number of vulnerabilities we create in the development process, our users are safer by default. We believe this is the most scalable approach to building resilient software.

Third, we know that when a vulnerability does surface in our products, it's important to issue fixes quickly and to be transparent. We believe that vendors should seek to reduce the burden on end-users by making it as easy as possible to apply software updates. Google Chrome and Google ChromeOS, for example, automatically update on behalf of the user so they are protected as soon as possible. We know the speed of deployment of patches is crucial to reducing the attacker's chances of their success.

In the interest of transparency, we also issue CVEs and security bulletins for products that may require users to take action, including Android and Google Cloud. This transparency also gives external parties insights into the type of vulnerabilities we observe and address.

In addition to our internal proactive measures, we also collaborate with the industry and engage with the external research community. For example, via our Vulnerability Disclosure Policy and our Vulnerability Rewards Programs, we have connected with security researchers all over the world that have helped us secure the products. Since we launched these programs in 2010, we've distributed 18,500 awards totaling nearly US$59 million.

Finally, when users and businesses use our products, it's important to notify them about possible intrusions into their accounts and the best practices to stay safe. We do this via warnings in their Google account, just like a car dashboard might alert a driver to an issue with the engine. This allows users to check on the settings of their accounts using a checkup tool and also look at personalized recommendations.

Enterprise users using Workspace and Cloud also have access to logging information to triage the impact on their business. These dashboard alerts are available in our products by default for no additional cost.

This is just a brief overview of what we've done over the last 20 years, the dedication we have to incorporating Secure by Design at Google. We know our work is not done. Securing the digital ecosystem really is a continuous effort. It's a team sport. We need industry partners, policy makers, and security experts at the table.

So I thank you for holding this important hearing, and I look forward to your questions. Thank you.

[The prepared statement of Ms. Adkins follows:]

PREPARED STATEMENT OF HEATHER ADKINS

DECEMBER 5, 2024

Chairman Garbarino, Ranking Member Swalwell, and Members of the committee, thank you for the opportunity to speak with you today. My name is Heather Adkins, and I serve as vice president for security engineering at Google.

Billions of people today rely on technology in their daily lives—to run their businesses, to further their education, for entertainment and shopping, and much more. In this interconnected world, it's critical that we ensure technology systems are resilient to keep people safe. As we know from the news, that isn't always the case.

Throughout my career in cybersecurity, I have had a good vantage point from which to study how security breaches occur, and the succession of events that cause them. What I have learned is that whether a system is resilient or not is a question of whether it was designed properly—cybersecurity is an inherent property of a system, the same way safety is an inherent property of an automobile.

For this reason, for over 20 years, Google has pioneered a Secure by Design approach, embedding security into every phase of the software development life cycle—not just at the beginning or the end. This year, we published a detailed white paper (also attached) on our approach, titled "An Overview of Google's Commitment to Secure by Design," and my testimony today will share some highlights from our work.

First, we know that many attacks start with social engineering—where an attacker tricks a user into taking a harmful action. Americans lost $12.5 billion to phishing and scams in 2023 alone. To combat these kinds of threats Google has invested in bringing multi-factor authentication to all our users. Our journey dates back to 2010, when we launched Google Authenticator and 2-Step Verification for Google Workspace. Since then, we have expanded this to all our services, and worked with the FIDO Alliance—an industry coalition—to develop standardized hardware tokens that stop password phishing. This coalition has also developed an industry standard called passkeys—a passwordless sign-in experience, which has been used to authenticate users more than 1 billion times. The industry goal is to eliminate the password—a key design flaw on the internet that has persisted for decades.

Second, attackers exploit entire classes of vulnerabilities that stem from how software is written. We have been working to proactively reduce the incidence of these. Our approach starts with our safe coding frameworks and secure development environment. This means we give our developers the tools to write safe code by default, rather than relying on them to understand and remember everything about security.

We've been able to prevent many of MITRE's 25 Most Dangerous Software Weaknesses from entering our code base, such as cross-site scripting (the No. 1 weakness), SQL injection (the No. 3 weakness) and others. By reducing the number of vulnerabilities we create in our software development process, our users are safer by default. We believe this is the most scalable approach to building resilient software.

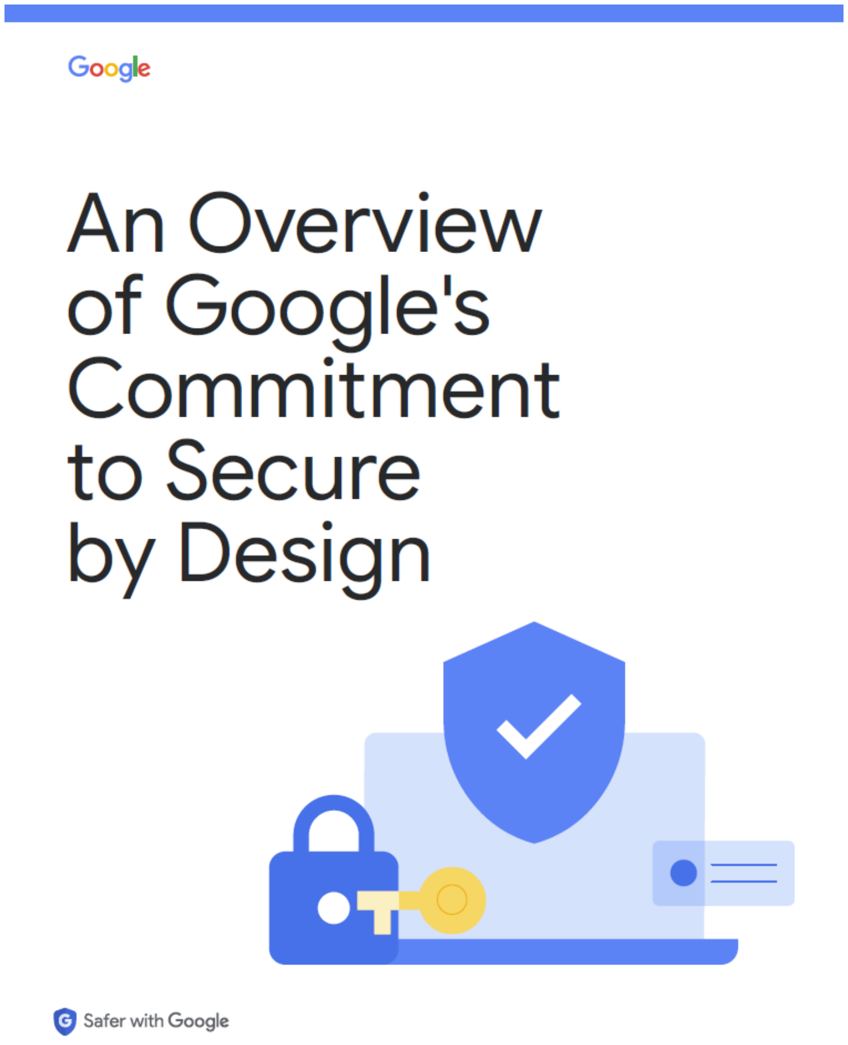
Third, we know that when a vulnerability does surface in our products it's important to issue fixes quickly and to be transparent. We also believe that vendors should seek to reduce the burden on end users by making it as easy as possible to apply software updates. Google Chrome and ChromeOS, for example, automatically update on the user's behalf so they are protected as soon as possible. We know the speed of deployment is crucial to reducing an attacker's chances of exploiting those flaws. In the interest of transparency, we issue Common Vulnerability and Exposure (CVEs) and security bulletins for products that may require consumers and business to take action, including Android, Google Cloud, and many others. This transparency gives external parties insights into the types of vulnerabilities we observe and address.

In addition to our internal proactive measures, Google collaborates across industry and extensively engages with the external research community, experts, and the public. For example, our Vulnerability Disclosure Policy and Vulnerability Rewards Programs have connected us to security researchers all over the world that have helped us to secure our products. Since we launched the Vulnerability Rewards Programs in 2010, we have distributed 18,500 rewards totaling nearly $59 million.

Finally, when users and businesses use our products, it's important that we notify them about possible intrusions into their accounts, and best practices on how to stay safe. We inform users via warnings about the security of their Google accounts, just as a car dashboard might alert the driver to an issue with the engine. This allows the user to check the settings of their account using our Security Checkup tool, which offers Security Alerts and personalized recommendations. Enterprise users using our Workspace and Cloud products also have access to useful logging information to triage the impact to their businesses. These “dashboard alerts” are available in our products by default, for no additional cost.

This is a brief overview of 20 years of dedication to incorporating Secure by Design at Google, but our work is not done. Securing our digital ecosystem is a continuous effort, and a team sport where we need industry partners, policy makers, and security experts at the table.

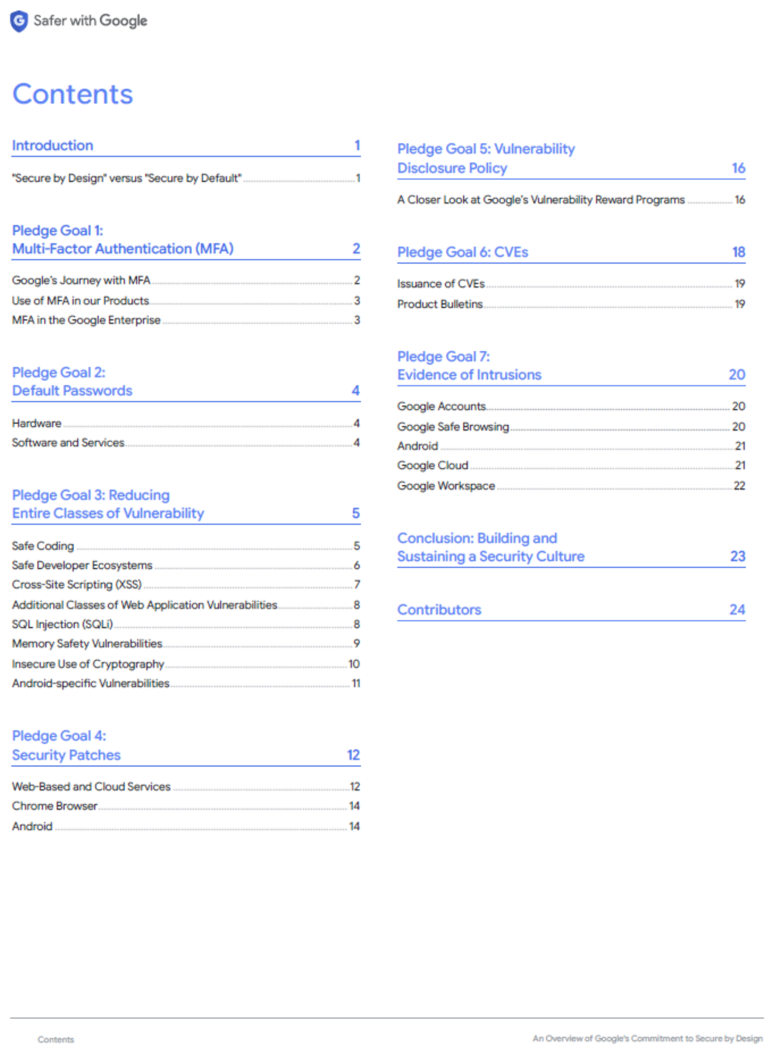
Thank you, again, for holding this important hearing. I look forward to answering your questions.



Google

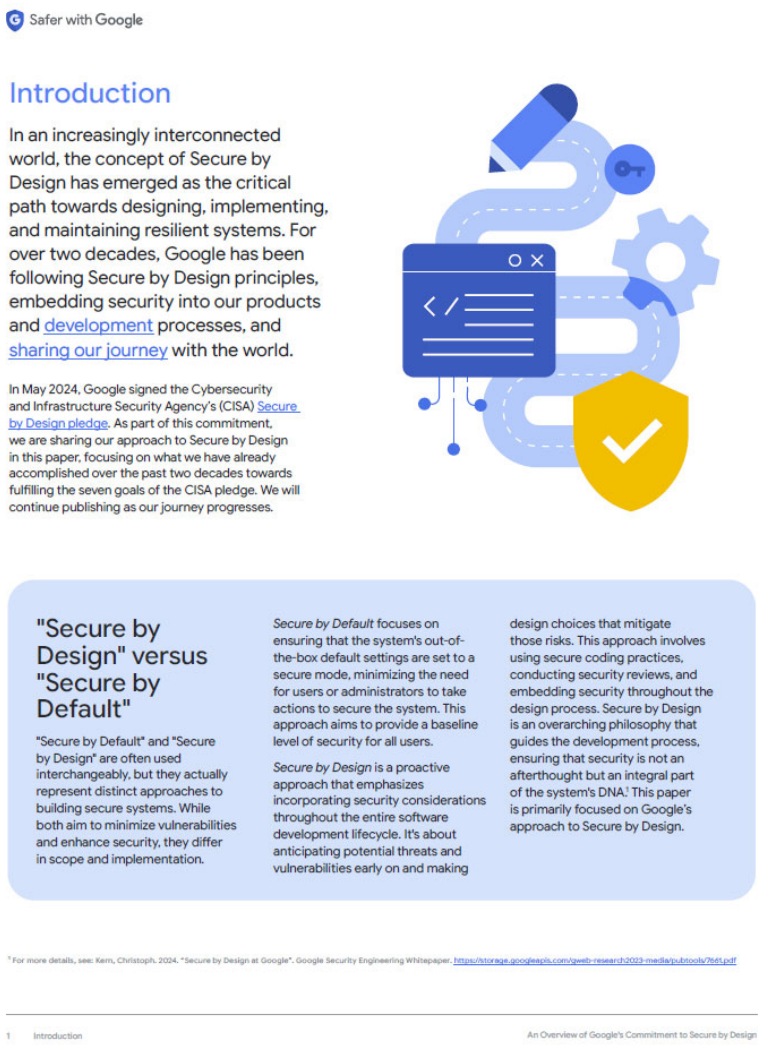
An Overview of Google's Commitment to Secure by Design

Safer with Google



Safer with Google

Contents



Safer with Google

Introduction

In an increasingly interconnected world, the concept of Secure by Design has emerged as the critical path towards designing, implementing, and maintaining resilient systems. For over two decades, Google has been following Secure by Design principles, embedding security into our products and development processes, and sharing our journey with the world.

In May 2024, Google signed the Cybersecurity and Infrastructure Security Agency's (CISA) Secure by Design pledge. As part of this commitment, we are sharing our approach to Secure by Design in this paper, focusing on what we have already accomplished over the past two decades towards fulfilling the seven goals of the CISA pledge. We will continue publishing as our journey progresses.

"Secure by Design" versus "Secure by Default"

"Secure by Default" and "Secure by Design" are often used interchangeably, but they actually represent distinct approaches to building secure systems. While both aim to minimize vulnerabilities and enhance security, they differ in scope and implementation.

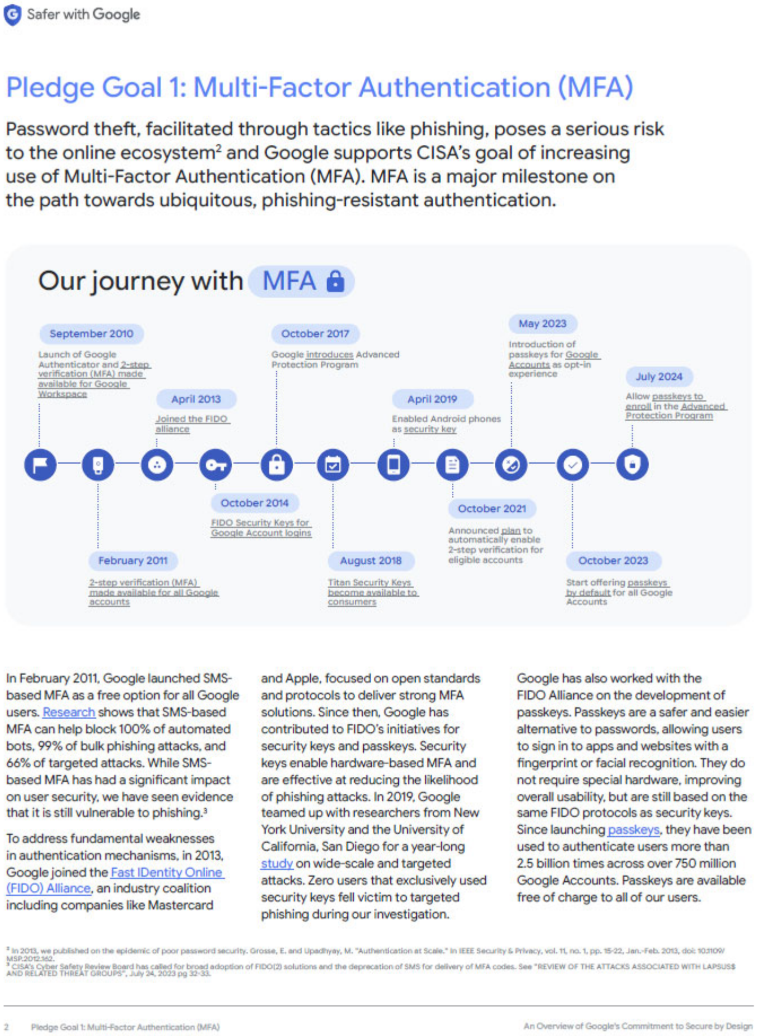
Secure by Default focuses on ensuring that the system's out-of-the-box default settings are set to a secure mode, minimizing the need for users or administrators to take actions to secure the system. This approach aims to provide a baseline level of security for all users.

Secure by Design is a proactive approach that emphasizes incorporating security considerations throughout the entire software development lifecycle. It's about anticipating potential threats and vulnerabilities early on and making design choices that mitigate those risks. This approach involves using secure coding practices, conducting security reviews, and embedding security throughout the design process. Secure by Design is an overarching philosophy that guides the development process, ensuring that security is not an afterthought but an integral part of the system's DNA.[1] This paper is primarily focused on Google's approach to Secure by Design.

[1] For more details, see: Kern, Christoph. 2024. "Secure by Design at Google". Google Security Engineering Whitepaper. https://storage.googleapis.com/gweb-research2023-media/pubtools/7661.pdf

1 Introduction

An Overview of Google's Commitment to Secure by Design



Pledge Goal 1: Multi-Factor Authentication (MFA)

Password theft, facilitated through tactics like phishing, poses a serious risk to the online ecosystem[2] and Google supports CISA's goal of increasing use of Multi-Factor Authentication (MFA). MFA is a major milestone on the path towards ubiquitous, phishing-resistant authentication.

Our journey with MFA

September 2010
Launch of Google Authenticator and 2-step verification (MFA) made available for Google Workspace

February 2011
2-step verification (MFA) made available for all Google accounts

April 2013
Joined the FIDO alliance

October 2014
FIDO Security Keys for Google Account logins

October 2017
Google introduces Advanced Protection Program

August 2018
Titan Security Keys become available to consumers

April 2019
Enabled Android phones as security key

October 2021
Announced plan to automatically enable 2-step verification for eligible accounts

May 2023
Introduction of passkeys for Google Accounts as opt-in experience

October 2023
Start offering passkeys by default for all Google Accounts

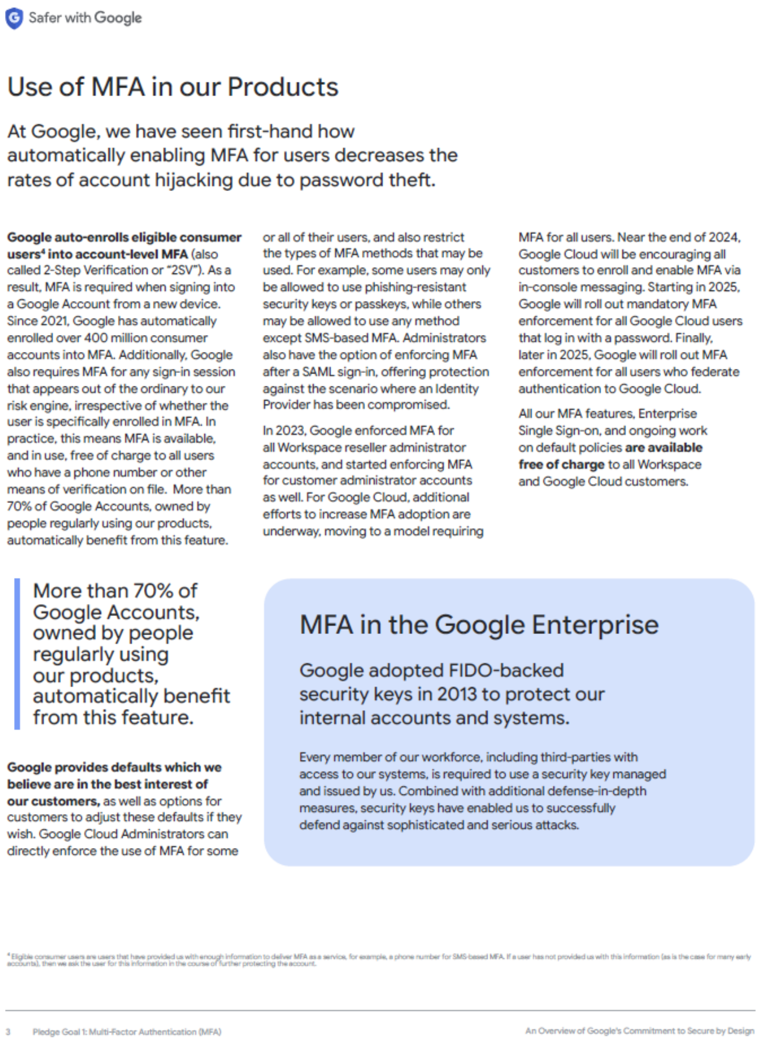
July 2024
Allow passkeys to enroll in the Advanced Protection Program

In February 2011, Google launched SMS-based MFA as a free option for all Google users. Research shows that SMS-based MFA can help block 100% of automated bots, 99% of bulk phishing attacks, and 66% of targeted attacks. While SMS-based MFA has had a significant impact on user security, we have seen evidence that it is still vulnerable to phishing.[3]

To address fundamental weaknesses in authentication mechanisms, in 2013, Google joined the Fast IDentity Online (FIDO) Alliance, an industry coalition including companies like Mastercard and Apple, focused on open standards and protocols to deliver strong MFA solutions. Since then, Google has contributed to FIDO's initiatives for security keys and passkeys. Security keys enable hardware-based MFA and are effective at reducing the likelihood of phishing attacks. In 2019, Google teamed up with researchers from New York University and the University of California, San Diego for a year-long study on wide-scale and targeted attacks. Zero users that exclusively used security keys fell victim to targeted phishing during our investigation.

Google has also worked with the FIDO Alliance on the development of passkeys. Passkeys are a safer and easier alternative to passwords, allowing users to sign in to apps and websites with a fingerprint or facial recognition. They do not require special hardware, improving overall usability, but are still based on the same FIDO protocols as security keys. Since launching passkeys, they have been used to authenticate users more than 2.5 billion times across over 750 million Google Accounts. Passkeys are available free of charge to all of our users.

[2] In 2013, we published on the epidemic of poor password security. Grosse, E. and Upadhyay, M. "Authentication at Scale." In IEEE Security & Privacy, vol. 11, no. 1, pp. 15-22, Jan.-Feb. 2013, doi: 10.1109/MSP.2012.162.
[3] CISA's Cyber Safety Review Board has called for broad adoption of FIDO(2) solutions and the deprecation of SMS for delivery of MFA codes. See "REVIEW OF THE ATTACKS ASSOCIATED WITH LAPSUS$ AND RELATED THREAT GROUPS", July 24, 2023 pg 32-33.



Use of MFA in our Products

At Google, we have seen first-hand how automatically enabling MFA for users decreases the rates of account hijacking due to password theft.

Google auto-enrolls eligible consumer users[4] into account-level MFA (also called 2-Step Verification or "2SV"). As a result, MFA is required when signing into a Google Account from a new device. Since 2021, Google has automatically enrolled over 400 million consumer accounts into MFA. Additionally, Google also requires MFA for any sign-in session that appears out of the ordinary to our risk engine, irrespective of whether the user is specifically enrolled in MFA. In practice, this means MFA is available, and in use, free of charge to all users who have a phone number or other means of verification on file. More than 70% of Google Accounts, owned by people regularly using our products, automatically benefit from this feature.

> More than 70% of Google Accounts, owned by people regularly using our products, automatically benefit from this feature.

Google provides defaults which we believe are in the best interest of our customers, as well as options for customers to adjust these defaults if they wish. Google Cloud Administrators can directly enforce the use of MFA for some or all of their users, and also restrict the types of MFA methods that may be used. For example, some users may only be allowed to use phishing-resistant security keys or passkeys, while others may be allowed to use any method except SMS-based MFA. Administrators also have the option of enforcing MFA after a SAML sign-in, offering protection against the scenario where an Identity Provider has been compromised.

In 2023, Google enforced MFA for all Workspace reseller administrator accounts, and started enforcing MFA for customer administrator accounts as well. For Google Cloud, additional efforts to increase MFA adoption are underway, moving to a model requiring MFA for all users. Near the end of 2024, Google Cloud will be encouraging all customers to enroll and enable MFA via in-console messaging. Starting in 2025, Google will roll out mandatory MFA enforcement for all Google Cloud users that log in with a password. Finally, later in 2025, Google will roll out MFA enforcement for all users who federate authentication to Google Cloud.

All our MFA features, Enterprise Single Sign-on, and ongoing work on default policies **are available free of charge** to all Workspace and Google Cloud customers.

MFA in the Google Enterprise

Google adopted FIDO-backed security keys in 2013 to protect our internal accounts and systems.

Every member of our workforce, including third-parties with access to our systems, is required to use a security key managed and issued by us. Combined with additional defense-in-depth measures, security keys have enabled us to successfully defend against sophisticated and serious attacks.

[4] Eligible consumer users are users that have provided us with enough information to deliver MFA as a service, for example, a phone number for SMS-based MFA. If a user has not provided us with this information (as is the case for many early accounts), then we ask the user for this information in the course of further protecting the account.

Pledge Goal 2: Default Passwords

Default passwords used in software and hardware can be easily discovered by threat actors. This basic vulnerability is an area Google has addressed by implementing best practices across our hardware and software ecosystem, and including it as a component of our security reviews. If a default password was present in our products, we would treat that as a vulnerability and handle it through our established processes for remediating issues.

Hardware

When designing retail hardware-based product lines, Google uses a system setup and maintenance life cycle that links the device to the user's Google account and does not rely on preconfigured passwords on these devices. For instance, configuring a new Nest smart home device, Google Pixel phone, Google TV streamer, or Fitbit wearable requires the user to log in with an individual Google account. Additionally, smart home device setup using a mobile app such as Google Nest or Google Home requires the device to be within Bluetooth range of the mobile phone and the device needs to be on the local WiFi network. For devices like Google Nest cameras, routers, and Chromecast streamers, a code on the device (e.g., a QR code) needs to be scanned or typed in by the user to prove physical possession before being able to link the product to a home data structure.

Smart home devices are managed by the user via a Google mobile app (e.g., Nest, Google Home) and can be accessed via the mobile app or a Web app. This access relies on a Google account and device linking, not on default passwords. In addition, there is no support for remote administration, for example, in a corporate environment. Factory reset logic is available and allows the user in possession of the device to wipe user data and unlink devices from their account. Return Merchandise Authorization (RMA) servicing for these devices uses factory reset within processes defined by Google. Similarly, RMA for Pixel devices is driven by systems owned by Google that enable an RMA agent to safely handle returned devices, including the removal of user data and factory reset.

Software and Services

Google's software-based services are similarly set up and accessed using a Google Account. Enterprise Cloud-based services such as Workspace and Google Cloud are managed by organization administrators. The setup process for these accounts does not involve default passwords. Cloud-based API services leverage a centralized Cloud IAM service that relies on industry-standard authentication mechanisms (e.g., OAuth 2.0, OpenID Connect), eliminating the need for additional credentials. When a domain administrator creates a new user in the Google Workspace Admin Console, Google automatically generates a strong password.

Pledge Goal 3: Reducing Entire Classes of Vulnerability

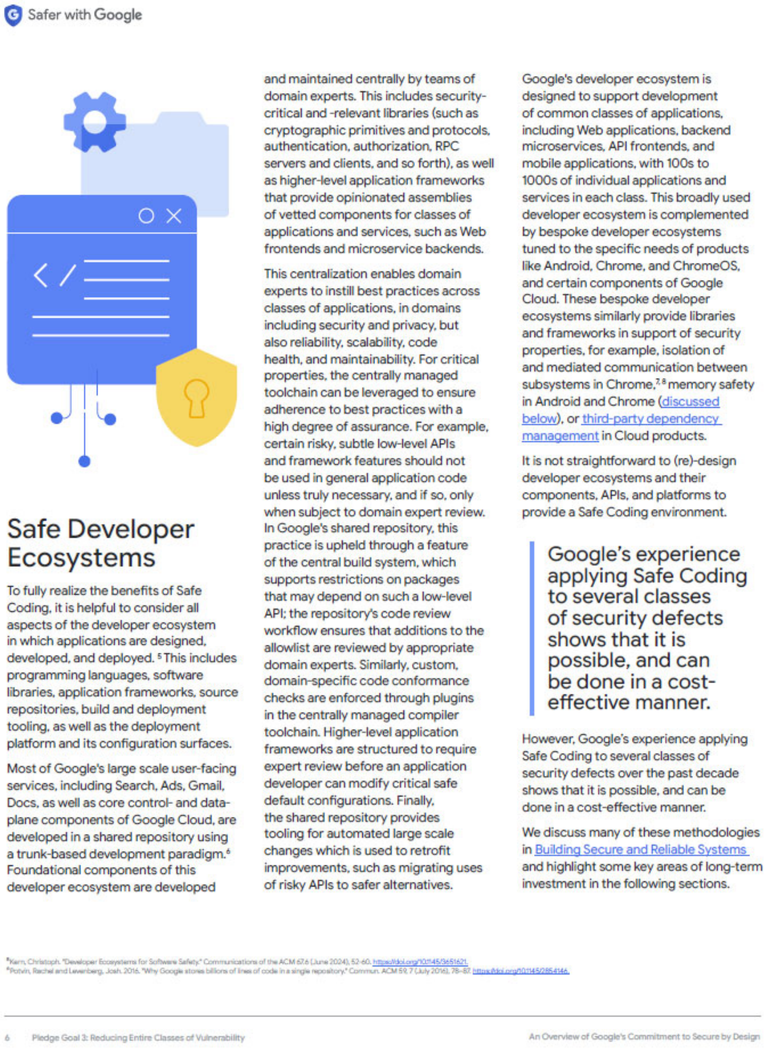
Google's products and services are built on top of platforms, such as our custom production environment, Google Cloud, and Android, as well as platforms defined by public standards, like the Web Platform and foundational Internet protocols, all of which have enabled our ability to address vulnerabilities at scale over time. As part of our platform work, Google has built simple, safe, and reliable libraries, abstractions, and application frameworks for our developers to use with the goal of eliminating classes of vulnerabilities in the code they write.

Safe Coding

The principle of Safe Coding is based on the idea that APIs and platform features should be inherently safe in any reasonable usage, and not only when developers carefully adhere to complex and difficult-to-reason-about secure-coding guidelines. A key observation informing the Safe Coding approach is that common classes of vulnerabilities in software applications tend to arise from the design of APIs, libraries, and platforms that developers use when building and deploying these applications. The design of an API or platform feature can be inherently risky, in that it requires the developer to carefully write the code that uses the API so as to ensure a critical security property or invariant; if the developer makes a subtle mistake and their code fails to ensure the security property, an exploitable vulnerability might be present.

In other words, each use of the risky API or platform feature in question is potentially vulnerable, unless the developer carefully adhered to secure-coding and -configuration guidelines and avoided making any mistake. Given a substantial number of potential vulnerabilities, some actual vulnerabilities tend to sneak into code or configuration. And once a vulnerability has been introduced, efforts to discover and fix it (such as code review, static or dynamic code analysis) are inherently incomplete and unable to find every single instance.

At Google, we've found that the most effective approach to address classes of vulnerabilities due to potentially pervasive coding or configuration errors (such as bugs in code relying on widely-used APIs or platform features) is to replace risky, mistake-prone APIs and platform features with functionally equivalent APIs that are designed to be safe by design, and which protect developers from the risk of accidentally introducing vulnerabilities – thereby enabling Safe Coding.



Safe Developer Ecosystems

To fully realize the benefits of Safe Coding, it is helpful to consider all aspects of the developer ecosystem in which applications are designed, developed, and deployed.[5] This includes programming languages, software libraries, application frameworks, source repositories, build and deployment tooling, as well as the deployment platform and its configuration surfaces.

Most of Google's large scale user-facing services, including Search, Ads, Gmail, Docs, as well as core control- and data-plane components of Google Cloud, are developed in a shared repository using a trunk-based development paradigm.[6] Foundational components of this developer ecosystem are developed and maintained centrally by teams of domain experts. This includes security-critical and -relevant libraries (such as cryptographic primitives and protocols, authentication, authorization, RPC servers and clients, and so forth), as well as higher-level application frameworks that provide opinionated assemblies of vetted components for classes of applications and services, such as Web frontends and microservice backends.

This centralization enables domain experts to instill best practices across classes of applications, in domains including security and privacy, but also reliability, scalability, code health, and maintainability. For critical properties, the centrally managed toolchain can be leveraged to ensure adherence to best practices with a high degree of assurance. For example, certain risky, subtle low-level APIs and framework features should not be used in general application code unless truly necessary, and if so, only when subject to domain expert review. In Google's shared repository, this practice is upheld through a feature of the central build system, which supports restrictions on packages that may depend on such a low-level API; the repository's code review workflow ensures that additions to the allowlist are reviewed by appropriate domain experts. Similarly, custom, domain-specific code conformance checks are enforced through plugins in the centrally managed compiler toolchain. Higher-level application frameworks are structured to require expert review before an application developer can modify critical safe default configurations. Finally, the shared repository provides tooling for automated large scale changes which is used to retrofit improvements, such as migrating uses of risky APIs to safer alternatives.

Google's developer ecosystem is designed to support development of common classes of applications, including Web applications, backend microservices, API frontends, and mobile applications, with 100s to 1000s of individual applications and services in each class. This broadly used developer ecosystem is complemented by bespoke developer ecosystems tuned to the specific needs of products like Android, Chrome, and ChromeOS, and certain components of Google Cloud. These bespoke developer ecosystems similarly provide libraries and frameworks in support of security properties, for example, isolation of and mediated communication between subsystems in Chrome,[7,8] memory safety in Android and Chrome (discussed below), or third-party dependency management in Cloud products.

It is not straightforward to (re)-design developer ecosystems and their components, APIs, and platforms to provide a Safe Coding environment.

> Google's experience applying Safe Coding to several classes of security defects shows that it is possible, and can be done in a cost-effective manner.

However, Google's experience applying Safe Coding to several classes of security defects over the past decade shows that it is possible, and can be done in a cost-effective manner.

We discuss many of these methodologies in Building Secure and Reliable Systems and highlight some key areas of long-term investment in the following sections.

[5] Kern, Christoph. "Developer Ecosystems for Software Safety." Communications of the ACM 67.6 (June 2024), 52-60. https://doi.org/10.1145/3651621.
[6] Potvin, Rachel and Levenberg, Josh. 2016. "Why Google stores billions of lines of code in a single repository." Commun. ACM 59, 7 (July 2016), 78–87. https://doi.org/10.1145/2854146.

Cross-Site Scripting (XSS)

Cross-site scripting (XSS) has been one of the major web security vulnerabilities for over a decade, ranking 2nd in the Stubborn Weaknesses in the CWE Top 25, and being the most commonly reported vulnerability class across several popular online bug bounty platforms. This is why Google focused on this vulnerability class and proactive measures to drastically reduce its occurrence in our major products. Because core web technologies allow unsafely mixing code and data (for example, HTML permits the loading of <script> elements which execute arbitrary JavaScript code alongside harmless presentational markup), XSS is common whenever developers compose web pages using data outside of their control without first escaping, sanitizing, or otherwise validating it. Any malicious scripts injected into a web page execute in users' browsers with the privileges of the affected web origin, giving the attacker full control over a user's session and allowing them to view or edit the user's data, or perform other malicious actions in the vulnerable application.

At Google, our approach to addressing XSS in sensitive services is two-fold and relies on hardening internal application development frameworks using the Safe Coding approach, and developing and enabling defense-in-depth anti-XSS mechanisms built directly into web browsers. Google's internal frameworks replace unsafe APIs with inherently secure alternatives, such as those provided by strictly autoescaping template systems or client-side frameworks, such as the safevalues library. These safe APIs are designed to ensure the absence of specific vulnerability classes and their usage is verified during compile-time (e.g., through tools such as the safety-web plugin and internal equivalents).

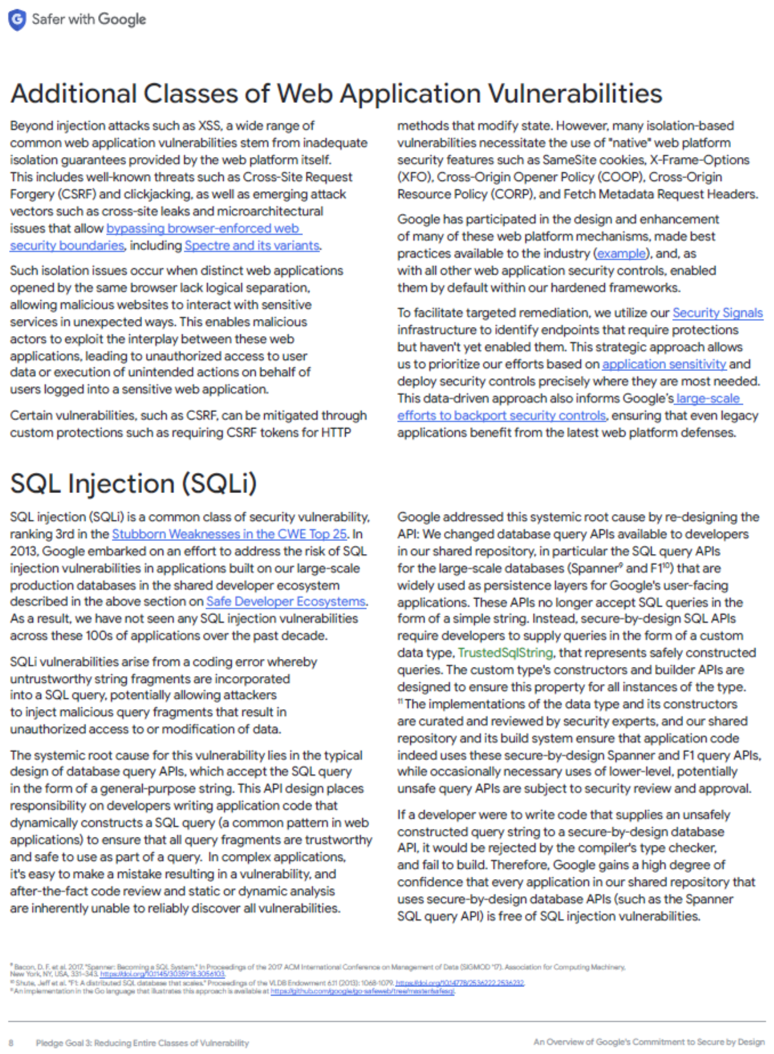
Our hardened web frameworks enable these protections by default and are designed to prevent developers from disabling them without undergoing a review by security experts.

To complement these compile-time security features, Google's application development frameworks also make use of core web platform defenses enforced at run-time by users' browsers, such as Content Security Policy and Trusted Types. Google actively collaborates with the W3C and web browser makers to develop and enhance these web platform security features and enable them by default for all of our recommended application development frameworks. Furthermore, Google proactively backports these security features at scale to protect existing applications (brownfield applications) from XSS vulnerabilities. This ensures that even applications launched before the widespread adoption of safe defaults benefit from enhanced security measures.

These compile-time and run-time security controls work together to provide defense-in-depth protection against XSS in sensitive services, ensuring that even if one security mechanism were to fail, others remain active and will prevent or mitigate the impact of a vulnerability. Data supports the conclusion that our proactive approach to addressing XSS has been highly effective. In the past three years, **for hundreds of complex web applications that are built on Google's hardened and safe-by-design frameworks, we've averaged less than one XSS report per year in total**. As an example, Google Photos was developed on secure-by-design frameworks from the outset, and has had no XSS vulnerabilities discovered in its codebase during its full lifetime. Additionally, by proactively backporting these security features at scale to existing applications, we've reduced XSS vulnerabilities in core Google products by 90% over the past decade.

> Google focused on this vulnerability class and proactive measures to drastically reduce its occurrence in our major products.

[7] Barth, Adam et al. 2008. "The security architecture of the Chromium browser." Technical report. Stanford University. https://seclab.stanford.edu/websec/chromium/chromium-security-architecture.pdf.
[8] Reis, Charles et al. 2019. "Site isolation: Process separation for web sites within the browser." 28th USENIX Security Symposium (USENIX Security 19).https://www.usenix.org/system/files/sec19-reis.pdf.



Additional Classes of Web Application Vulnerabilities

Beyond injection attacks such as XSS, a wide range of common web application vulnerabilities stem from inadequate isolation guarantees provided by the web platform itself. This includes well-known threats such as Cross-Site Request Forgery (CSRF) and clickjacking, as well as emerging attack vectors such as cross-site leaks and microarchitectural issues that allow bypassing browser-enforced web security boundaries, including Spectre and its variants.

Such isolation issues occur when distinct web applications opened by the same browser lack logical separation, allowing malicious websites to interact with sensitive services in unexpected ways. This enables malicious actors to exploit the interplay between these web applications, leading to unauthorized access to user data or execution of unintended actions on behalf of users logged into a sensitive web application.

Certain vulnerabilities, such as CSRF, can be mitigated through custom protections such as requiring CSRF tokens for HTTP methods that modify state. However, many isolation-based vulnerabilities necessitate the use of "native" web platform security features such as SameSite cookies, X-Frame-Options (XFO), Cross-Origin Opener Policy (COOP), Cross-Origin Resource Policy (CORP), and Fetch Metadata Request Headers.

Google has participated in the design and enhancement of many of these web platform mechanisms, made best practices available to the industry (example), and, as with all other web application security controls, enabled them by default within our hardened frameworks.

To facilitate targeted remediation, we utilize our Security Signals infrastructure to identify endpoints that require protections but haven't yet enabled them. This strategic approach allows us to prioritize our efforts based on application sensitivity and deploy security controls precisely where they are most needed. This data-driven approach also informs Google's large-scale efforts to backport security controls, ensuring that even legacy applications benefit from the latest web platform defenses.

SQL Injection (SQLi)

SQL injection (SQLi) is a common class of security vulnerability, ranking 3rd in the Stubborn Weaknesses in the CWE Top 25. In 2013, Google embarked on an effort to address the risk of SQL injection vulnerabilities in applications built on our large-scale production databases in the shared developer ecosystem described in the above section on Safe Developer Ecosystems. As a result, we have not seen any SQL injection vulnerabilities across these 100s of applications over the past decade.

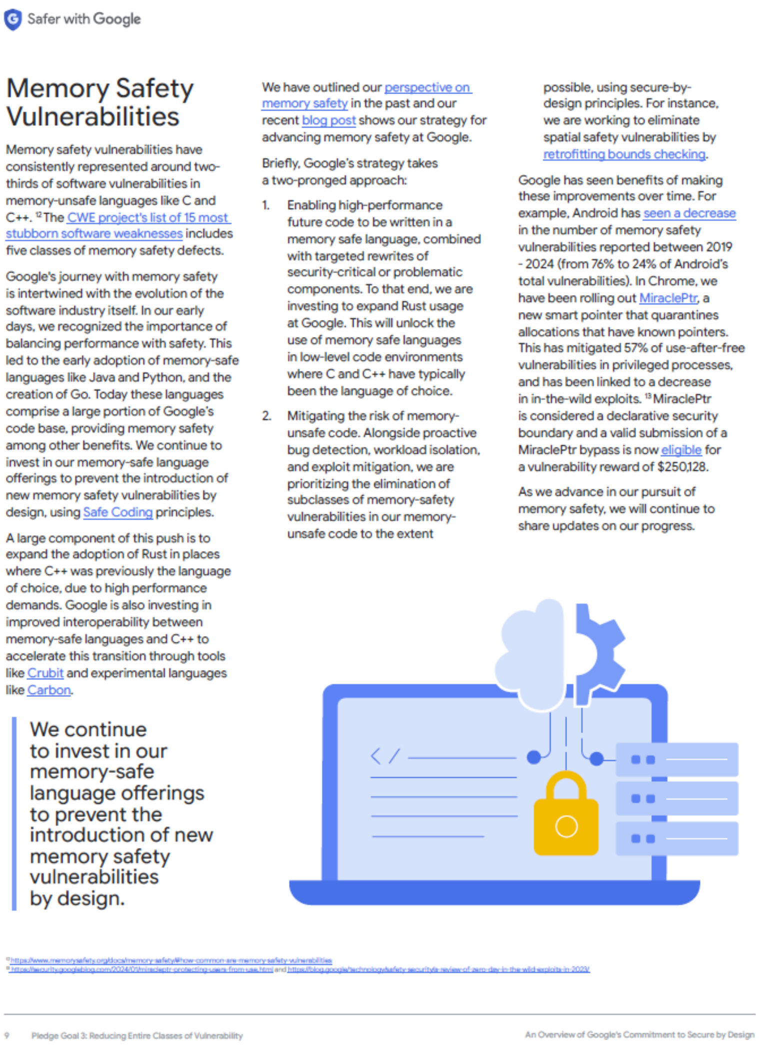
SQLi vulnerabilities arise from a coding error whereby untrustworthy string fragments are incorporated into a SQL query, potentially allowing attackers to inject malicious query fragments that result in unauthorized access to or modification of data.

The systemic root cause for this vulnerability lies in the typical design of database query APIs, which accept the SQL query in the form of a general-purpose string. This API design places responsibility on developers writing application code that dynamically constructs a SQL query (a common pattern in web applications) to ensure that all query fragments are trustworthy and safe to use as part of a query. In complex applications, it's easy to make a mistake resulting in a vulnerability, and after-the-fact code review and static or dynamic analysis are inherently unable to reliably discover all vulnerabilities.

Google addressed this systemic root cause by re-designing the API: We changed database query APIs available to developers in our shared repository, in particular the SQL query APIs for the large-scale databases (Spanner[9] and F1[10]) that are widely used as persistence layers for Google's user-facing applications. These APIs no longer accept SQL queries in the form of a simple string. Instead, secure-by-design SQL APIs require developers to supply queries in the form of a custom data type, TrustedSqlString, that represents safely constructed queries. The custom type's constructors and builder APIs are designed to ensure this property for all instances of the type.[11] The implementations of the data type and its constructors are curated and reviewed by security experts, and our shared repository and its build system ensure that application code indeed uses these secure-by-design Spanner and F1 query APIs, while occasionally necessary uses of lower-level, potentially unsafe query APIs are subject to security review and approval.

If a developer were to write code that supplies an unsafely constructed query string to a secure-by-design database API, it would be rejected by the compiler's type checker, and fail to build. Therefore, Google gains a high degree of confidence that every application in our shared repository that uses secure-by-design database APIs (such as the Spanner SQL query API) is free of SQL injection vulnerabilities.

[9] Bacon, D. F. et al. 2017. "Spanner: Becoming a SQL System." In Proceedings of the 2017 ACM International Conference on Management of Data (SIGMOD '17). Association for Computing Machinery, New York, NY, USA, 331–343. https://doi.org/10.1145/3035918.3056103.
[10] Shute, Jeff et al. "F1: A distributed SQL database that scales." Proceedings of the VLDB Endowment 6.11 (2013): 1068-1079. https://doi.org/10.14778/2536222.2536232.
[11] An implementation in the Go language that illustrates this approach is available at https://github.com/google/go-safeweb/tree/master/safesql.



Memory Safety Vulnerabilities

Memory safety vulnerabilities have consistently represented around two-thirds of software vulnerabilities in memory-unsafe languages like C and C++. [12] The CWE project's list of 15 most stubborn software weaknesses includes five classes of memory safety defects.

Google's journey with memory safety is intertwined with the evolution of the software industry itself. In our early days, we recognized the importance of balancing performance with safety. This led to the early adoption of memory-safe languages like Java and Python, and the creation of Go. Today these languages comprise a large portion of Google's code base, providing memory safety among other benefits. We continue to invest in our memory-safe language offerings to prevent the introduction of new memory safety vulnerabilities by design, using Safe Coding principles.

A large component of this push is to expand the adoption of Rust in places where C++ was previously the language of choice, due to high performance demands. Google is also investing in improved interoperability between memory-safe languages and C++ to accelerate this transition through tools like Crubit and experimental languages like Carbon.

> We continue to invest in our memory-safe language offerings to prevent the introduction of new memory safety vulnerabilities by design.

We have outlined our perspective on memory safety in the past and our recent blog post shows our strategy for advancing memory safety at Google.

Briefly, Google's strategy takes a two-pronged approach:

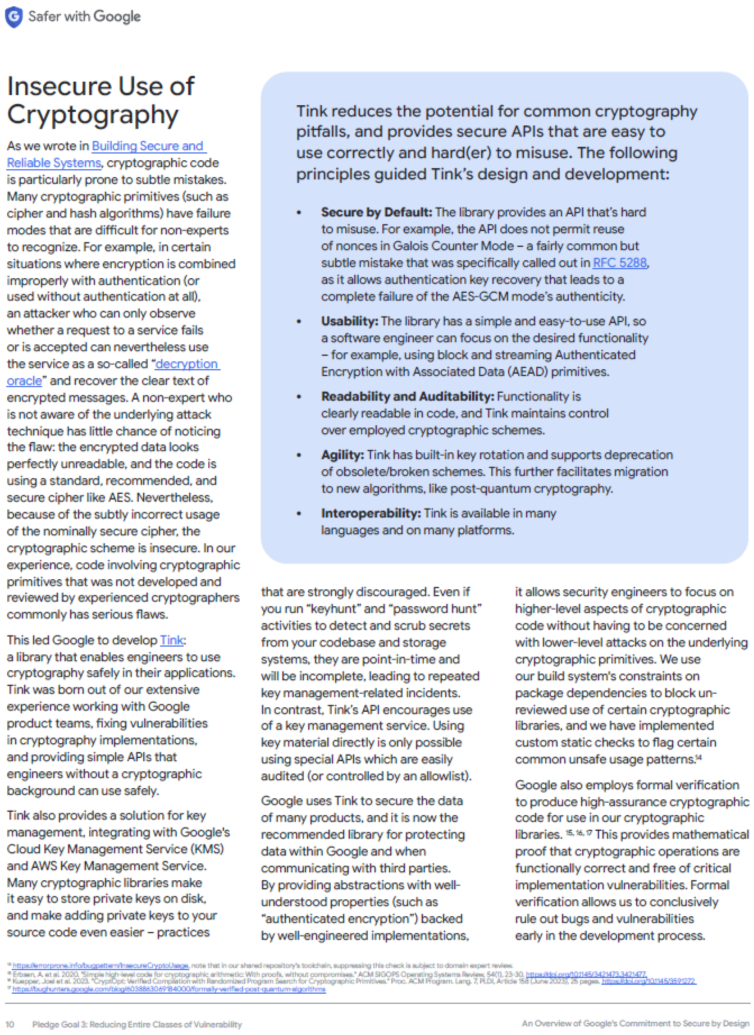
1. Enabling high-performance future code to be written in a memory safe language, combined with targeted rewrites of security-critical or problematic components. To that end, we are investing to expand Rust usage at Google. This will unlock the use of memory safe languages in low-level code environments where C and C++ have typically been the language of choice.
2. Mitigating the risk of memory-unsafe code. Alongside proactive bug detection, workload isolation, and exploit mitigation, we are prioritizing the elimination of subclasses of memory-safety vulnerabilities in our memory-unsafe code to the extent possible, using secure-by-design principles. For instance, we are working to eliminate spatial safety vulnerabilities by retrofitting bounds checking.

Google has seen benefits of making these improvements over time. For example, Android has seen a decrease in the number of memory safety vulnerabilities reported between 2019 - 2024 (from 76% to 24% of Android's total vulnerabilities). In Chrome, we have been rolling out MiraclePtr, a new smart pointer that quarantines allocations that have known pointers. This has mitigated 57% of use-after-free vulnerabilities in privileged processes, and has been linked to a decrease in in-the-wild exploits. [13] MiraclePtr is considered a declarative security boundary and a valid submission of a MiraclePtr bypass is now eligible for a vulnerability reward of $250,128.

As we advance in our pursuit of memory safety, we will continue to share updates on our progress.

[12] https://www.memorysafety.org/docs/memory-safety/#how-common-are-memory-safety-vulnerabilities

[13] https://security.googleblog.com/2024/01/miracleptr-protecting-users-from-use.html and https://blog.google/technology/safety-security/a-review-of-zero-day-in-the-wild-exploits-in-2023/



Safer with Google

Insecure Use of Cryptography

As we wrote in Building Secure and Reliable Systems, cryptographic code is particularly prone to subtle mistakes. Many cryptographic primitives (such as cipher and hash algorithms) have failure modes that are difficult for non-experts to recognize. For example, in certain situations where encryption is combined improperly with authentication (or used without authentication at all), an attacker who can only observe whether a request to a service fails or is accepted can nevertheless use the service as a so-called "decryption oracle" and recover the clear text of encrypted messages. A non-expert who is not aware of the underlying attack technique has little chance of noticing the flaw: the encrypted data looks perfectly unreadable, and the code is using a standard, recommended, and secure cipher like AES. Nevertheless, because of the subtly incorrect usage of the nominally secure cipher, the cryptographic scheme is insecure. In our experience, code involving cryptographic primitives that was not developed and reviewed by experienced cryptographers commonly has serious flaws.

This led Google to develop Tink: a library that enables engineers to use cryptography safely in their applications. Tink was born out of our extensive experience working with Google product teams, fixing vulnerabilities in cryptography implementations, and providing simple APIs that engineers without a cryptographic background can use safely.

Tink reduces the potential for common cryptography pitfalls, and provides secure APIs that are easy to use correctly and hard(er) to misuse. The following principles guided Tink's design and development:

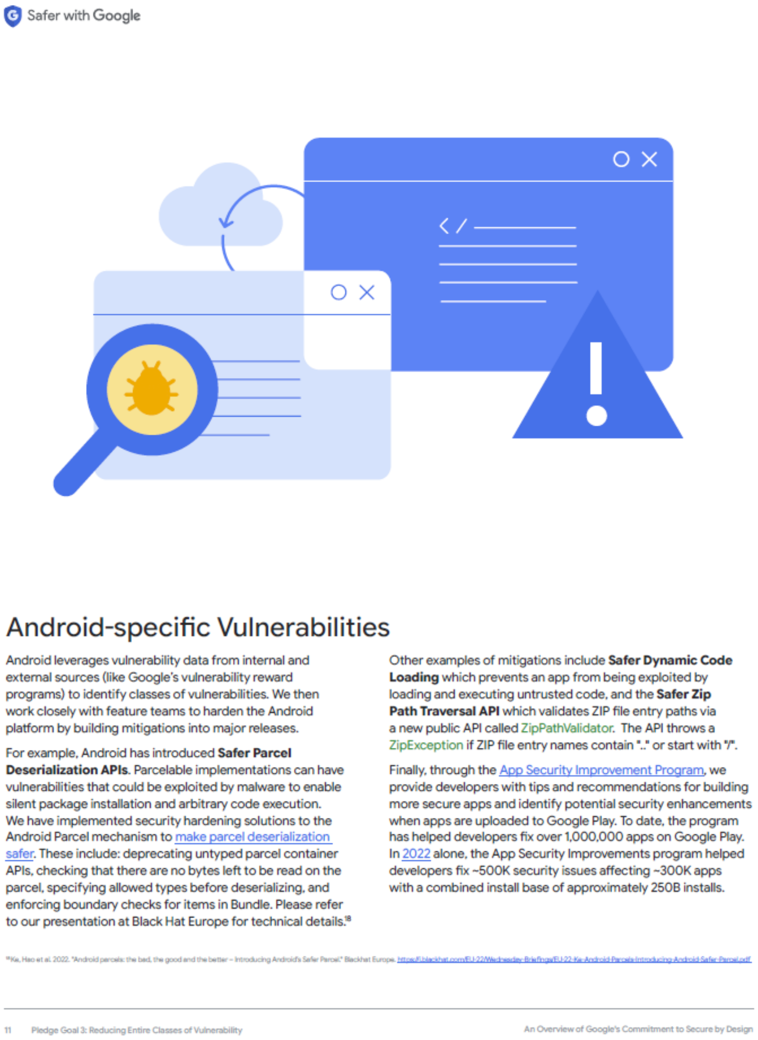
- **Secure by Default:** The library provides an API that's hard to misuse. For example, the API does not permit reuse of nonces in Galois Counter Mode – a fairly common but subtle mistake that was specifically called out in RFC 5288, as it allows authentication key recovery that leads to a complete failure of the AES-GCM mode's authenticity.
- **Usability:** The library has a simple and easy-to-use API, so a software engineer can focus on the desired functionality – for example, using block and streaming Authenticated Encryption with Associated Data (AEAD) primitives.
- **Readability and Auditability:** Functionality is clearly readable in code, and Tink maintains control over employed cryptographic schemes.
- **Agility:** Tink has built-in key rotation and supports deprecation of obsolete/broken schemes. This further facilitates migration to new algorithms, like post-quantum cryptography.
- **Interoperability:** Tink is available in many languages and on many platforms.

Tink also provides a solution for key management, integrating with Google's Cloud Key Management Service (KMS) and AWS Key Management Service. Many cryptographic libraries make it easy to store private keys on disk, and make adding private keys to your source code even easier – practices that are strongly discouraged. Even if you run "keyhunt" and "password hunt" activities to detect and scrub secrets from your codebase and storage systems, they are point-in-time and will be incomplete, leading to repeated key management-related incidents. In contrast, Tink's API encourages use of a key management service. Using key material directly is only possible using special APIs which are easily audited (or controlled by an allowlist).

Google uses Tink to secure the data of many products, and it is now the recommended library for protecting data within Google and when communicating with third parties. By providing abstractions with well-understood properties (such as "authenticated encryption") backed by well-engineered implementations, it allows security engineers to focus on higher-level aspects of cryptographic code without having to be concerned with lower-level attacks on the underlying cryptographic primitives. We use our build system's constraints on package dependencies to block un-reviewed use of certain cryptographic libraries, and we have implemented custom static checks to flag certain common unsafe usage patterns.[14]

Google also employs formal verification to produce high-assurance cryptographic code for use in our cryptographic libraries. [15, 16, 17] This provides mathematical proof that cryptographic operations are functionally correct and free of critical implementation vulnerabilities. Formal verification allows us to conclusively rule out bugs and vulnerabilities early in the development process.

[14] https://errorprone.info/bugpattern/InsecureCryptoUsage, note that in our shared repository's toolchain, suppressing this check is subject to domain expert review.
[15] Erbsen, A. et al. 2020. "Simple high-level code for cryptographic arithmetic: With proofs, without compromises." ACM SIGOPS Operating Systems Review, 54(1), 23-30. https://doi.org/10.1145/3421473.3421477.
[16] Kuepper, Joel et al. 2023. "CryptOpt: Verified Compilation with Randomized Program Search for Cryptographic Primitives." Proc. ACM Program. Lang. 7, PLDI, Article 158 (June 2023), 25 pages. https://doi.org/10.1145/3591272
[17] https://bughunters.google.com/blog/6038863069184000/formally-verified-post-quantum-algorithms



Android-specific Vulnerabilities

Android leverages vulnerability data from internal and external sources (like Google's vulnerability reward programs) to identify classes of vulnerabilities. We then work closely with feature teams to harden the Android platform by building mitigations into major releases.

For example, Android has introduced **Safer Parcel Deserialization APIs**. Parcelable implementations can have vulnerabilities that could be exploited by malware to enable silent package installation and arbitrary code execution. We have implemented security hardening solutions to the Android Parcel mechanism to make parcel deserialization safer. These include: deprecating untyped parcel container APIs, checking that there are no bytes left to be read on the parcel, specifying allowed types before deserializing, and enforcing boundary checks for items in Bundle. Please refer to our presentation at Black Hat Europe for technical details.[18]

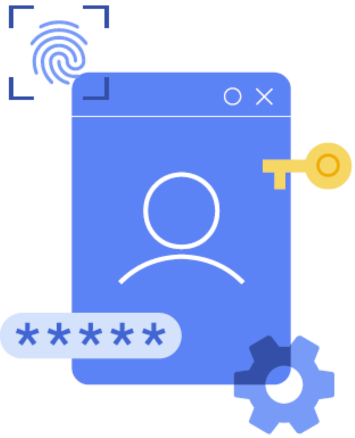
Other examples of mitigations include **Safer Dynamic Code Loading** which prevents an app from being exploited by loading and executing untrusted code, and the **Safer Zip Path Traversal API** which validates ZIP file entry paths via a new public API called ZipPathValidator. The API throws a ZipException if ZIP file entry names contain ".." or start with "/".

Finally, through the App Security Improvement Program, we provide developers with tips and recommendations for building more secure apps and identify potential security enhancements when apps are uploaded to Google Play. To date, the program has helped developers fix over 1,000,000 apps on Google Play. In 2022 alone, the App Security Improvements program helped developers fix ~500K security issues affecting ~300K apps with a combined install base of approximately 250B installs.

[18] Ke, Hao et al. 2022. "Android parcels: the bad, the good and the better – Introducing Android's Safer Parcel." Blackhat Europe. https://i.blackhat.com/EU-22/Wednesday-Briefings/EU-22-Ke-Android-Parcels-Introducing-Android-Safer-Parcel.pdf

Pledge Goal 4: Security Patches

While Google strives to minimize the number of issues in our products before they are released, we do know that errors – whether they're related to functionality, reliability, or security – are inevitable when building complex systems. We understand that addressing issues in our products is critical to their ongoing trustworthiness, and the trust pact with our users. As such, Google has developed strategies over time to ensure high rates of uptake for our deployed fixes, especially in cases where reducing the window of opportunity for exploitation is safety critical. We describe some examples below.



Web-Based and Cloud Services

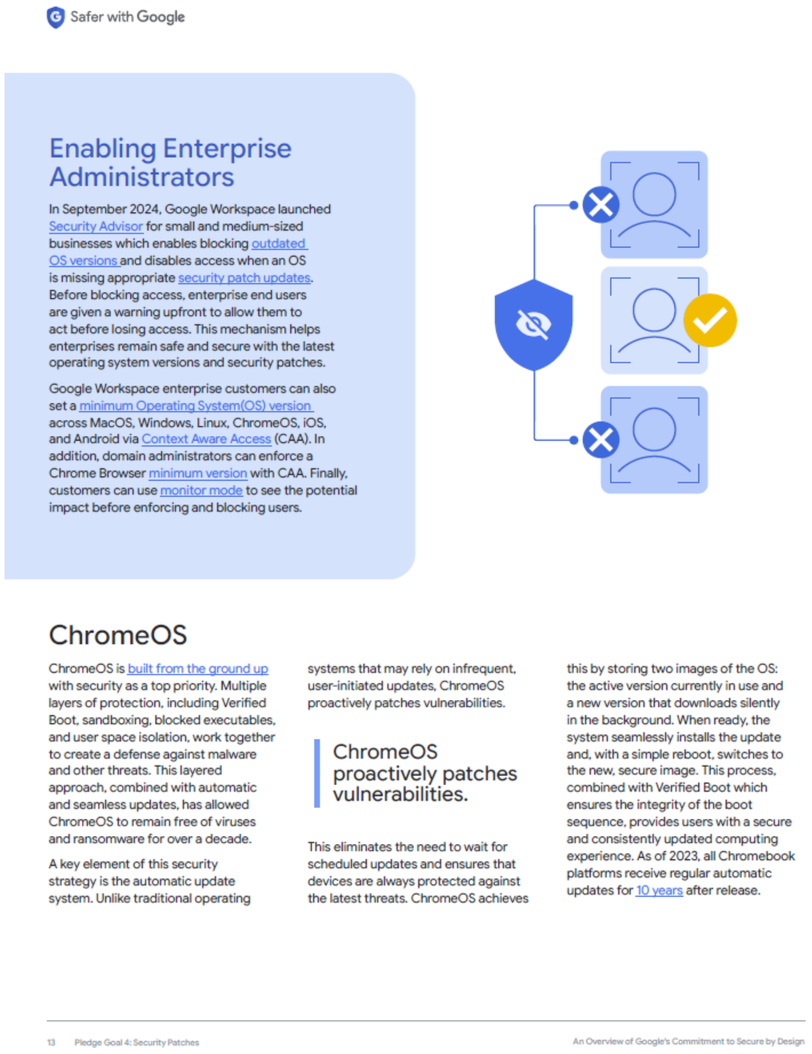
Many of Google's products are delivered through web-based services. These include some of our most widely used and popular products such as Search, YouTube, and Gmail. One benefit of online web-based services is that end-users and customers do not need to take any action to update the software should a vulnerability occur. As such, when Google deploys a fix for a functionality-, reliability-, or security-related issue, it is addressed for our entire user base once fully deployed according to our safe release procedures.

When developers run on top of the managed Google Cloud platform, they gain the same benefits:

Google can take responsibility for patching and updating the infrastructure they run on, so they and their end users benefit from the scalability and immediacy of a central solution.

For example, Google Cloud was able to protect all hosted developers from the Spectre and Meltdown vulnerabilities without action on their part.

We developed shared fate in Google Cloud to start addressing the challenges that the shared responsibility model doesn't address. Shared fate focuses on how all parties can better interact to continuously improve security. Shared fate builds on the shared responsibility model because it views the relationship between cloud provider and customer as an ongoing partnership to improve security.



Enabling Enterprise Administrators

In September 2024, Google Workspace launched Security Advisor for small and medium-sized businesses which enables blocking outdated OS versions and disables access when an OS is missing appropriate security patch updates. Before blocking access, enterprise end users are given a warning upfront to allow them to act before losing access. This mechanism helps enterprises remain safe and secure with the latest operating system versions and security patches.

Google Workspace enterprise customers can also set a minimum Operating System(OS) version across MacOS, Windows, Linux, ChromeOS, iOS, and Android via Context Aware Access (CAA). In addition, domain administrators can enforce a Chrome Browser minimum version with CAA. Finally, customers can use monitor mode to see the potential impact before enforcing and blocking users.

ChromeOS

ChromeOS is built from the ground up with security as a top priority. Multiple layers of protection, including Verified Boot, sandboxing, blocked executables, and user space isolation, work together to create a defense against malware and other threats. This layered approach, combined with automatic and seamless updates, has allowed ChromeOS to remain free of viruses and ransomware for over a decade.

A key element of this security strategy is the automatic update system. Unlike traditional operating systems that may rely on infrequent, user-initiated updates, ChromeOS proactively patches vulnerabilities.

> ChromeOS proactively patches vulnerabilities.

This eliminates the need to wait for scheduled updates and ensures that devices are always protected against the latest threats. ChromeOS achieves this by storing two images of the OS: the active version currently in use and a new version that downloads silently in the background. When ready, the system seamlessly installs the update and, with a simple reboot, switches to the new, secure image. This process, combined with Verified Boot which ensures the integrity of the boot sequence, provides users with a secure and consistently updated computing experience. As of 2023, all Chromebook platforms receive regular automatic updates for 10 years after release.

Chrome Browser

Chrome updates happen in the background whether or not the browser is running. Restarting a running browser may be necessary to complete the update, but if no browser is running, Chrome will update without any user interaction. Chrome Browser was built with secure-by-design technology to provide security patches regularly and automatically to Chrome users, reducing the window of vulnerability for exploits.

Chrome Browser has a rapid release cycle that ensures security patches are deployed frequently, typically every week. This rapid response time helps address vulnerabilities promptly. Chrome moved from a two-weekly to a weekly security update cycle in 2023.

Android

Android is an open source operating system that powers both Google's Pixel product line and devices from hundreds of manufacturers worldwide. Device makers and carriers are responsible for deploying patches in their environment, and to facilitate consistency and speed of patch delivery, Android has worked closely with partners to develop safe mechanisms for updates.

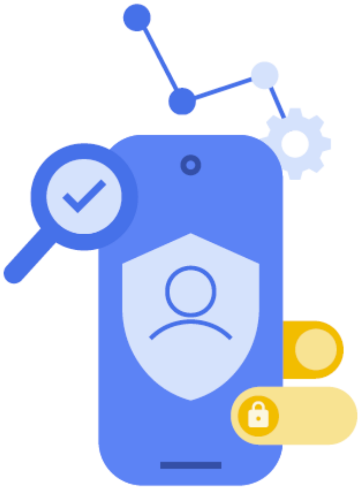
Android has instituted a Security Patch Level (SPL) that drives the ecosystem to patch devices regularly. Android issues regular partner preview bulletins (to drive patch adoption with partners), regular public security bulletins to inform users and the ecosystem of what patches are available, and advisories for high-risk issues. System updates with security fixes are pushed to user devices and staged for installation upon the next device reboot. Android also has mandatory requirements for real-time patching of emergency-class vulnerabilities.

Android also builds and maintains tooling to detect when partners are missing security patches and inform OEMs, as well as tooling, like Security Hub, to help users understand patch update status and other important security characteristics.

A key strategy in scaling security updates across a broad range of hardware products at varying price points is to make it easier and more cost-effective for device manufacturers to update software. To this end, Google has spent years rearchitecting Android, with a focus on increased compatibility and centralization of updates by Google.

> Google has spent years rearchitecting Android, with a focus on increased compatibility and centralization of updates by Google.

Major milestones of this journey include improving hardware compatibility across updates through Project Treble, and better collaboration with system-on-chip (SoC) manufacturers to deliver pre-tested system images via GMS Express (2017). In 2019, major Android components became Google-updateable through Project Mainline. Next, in 2020, Generic Kernel Image (GKI) unified the core kernel and moved hardware-specific code into loadable vendor modules, while Linux Protected KVM (pKVM) Hypervisor created a harmonized Android trusted execution environment (TEE). GKI was improved in 2021 with GKI 2.0, which requires signed kernel images that are patched regularly by Google with Long-Term Support (LTS) and critical bug fixes. In 2021, we also enabled standardized Android binaries for Secure Element (SE) applets, including over-the-air updates (Android ReadySE). Finally, in 2023 we introduced Android Virtualization Framework (AVF) to provide standardized interfaces for Android TEEs and virtual machines.



Pixel

Google's Pixel phones and watches powered by Android are designed to prioritize security and provide users with the latest features through automatic updates. In enterprise environments, IT administrators have the option to disable automatic updates, allowing them to test new software versions before deploying them across their fleet of Pixel phones. This flexibility ensures compatibility and minimizes potential disruptions.

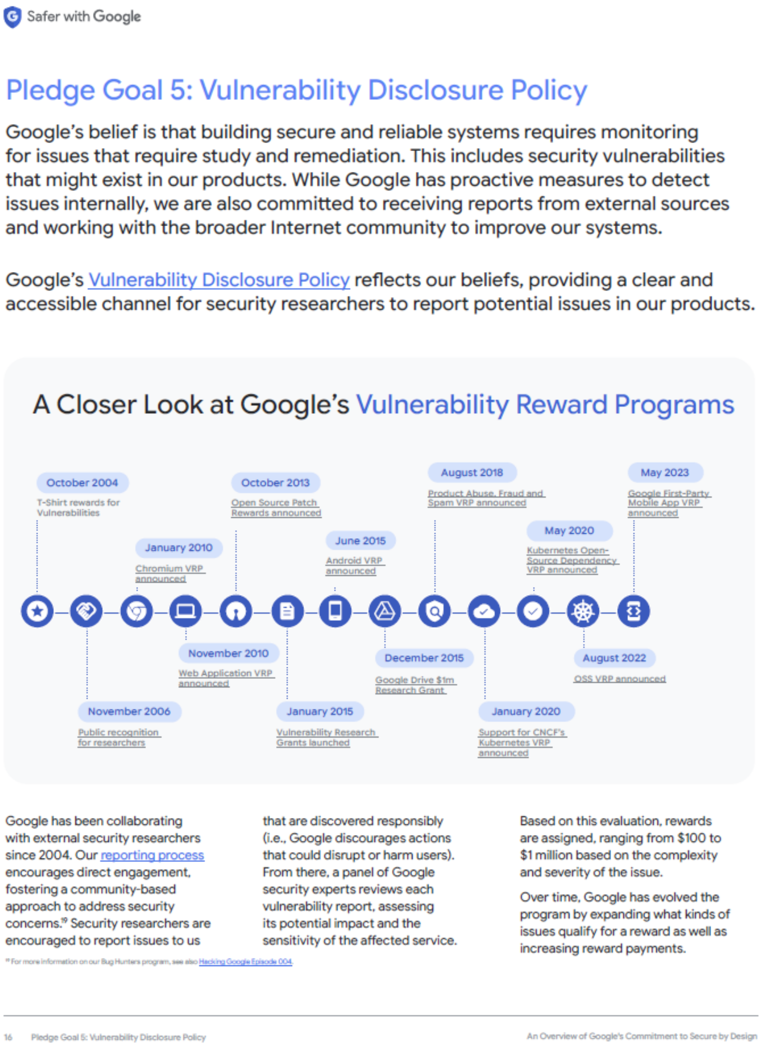
Additionally, Google maintains transparency by publishing Pixel security phone, tablet and watch bulletins and the security support periods for Pixel phones and watches, empowering users to make informed decisions about their devices' lifespan and ongoing protection. Software updates for Pixel customers are released regularly and include security patches. This rollout proceeds gradually and the updates become available to 100% of customers within two weeks. The latest Pixel 9 family of devices are guaranteed Android and security updates until at least August 2031.

Fitbit

While automatic updates are the easiest way to keep devices updated, things get far more complicated in highly constrained devices. For Fitbit trackers, these devices are small in size, but need to last a long time before getting charged. Thus, automatically pushing an update to the device could result in a failed update if the battery is not fully charged, or cause the device's battery to die at an inconvenient time for the user. Therefore, for these devices, the user is notified that an update is available, but the user controls when it is applied.

Nest

In 2019, Nest established a set of security and privacy commitments, further strengthened in 2021 by guaranteeing that all Nest devices will receive automatic security updates for a minimum of 5 years. Google deploys updates in a rolling fashion, which typically complete within a three-week period, and publishes the security support periods for each Nest device, enabling users to make informed decisions. Additionally, Google collaborates with security researchers who play a vital role in identifying vulnerabilities in our devices. Upon discovery and confirmation of a risk to users, these vulnerabilities are promptly patched, and the corresponding updates are automatically deployed to safeguard our users' homes and data.



Pledge Goal 5: Vulnerability Disclosure Policy

Google's belief is that building secure and reliable systems requires monitoring for issues that require study and remediation. This includes security vulnerabilities that might exist in our products. While Google has proactive measures to detect issues internally, we are also committed to receiving reports from external sources and working with the broader Internet community to improve our systems.

Google's Vulnerability Disclosure Policy reflects our beliefs, providing a clear and accessible channel for security researchers to report potential issues in our products.

A Closer Look at Google's Vulnerability Reward Programs

October 2004
T-Shirt rewards for Vulnerabilities

November 2006
Public recognition for researchers

January 2010
Chromium VRP announced

November 2010
Web Application VRP announced

October 2013
Open Source Patch Rewards announced

January 2015
Vulnerability Research Grants launched

June 2015
Android VRP announced

December 2015
Google Drive $1m Research Grant

August 2018
Product Abuse, Fraud and Spam VRP announced

January 2020
Support for CNCF's Kubernetes VRP announced

May 2020
Kubernetes Open-Source Dependency VRP announced

August 2022
OSS VRP announced

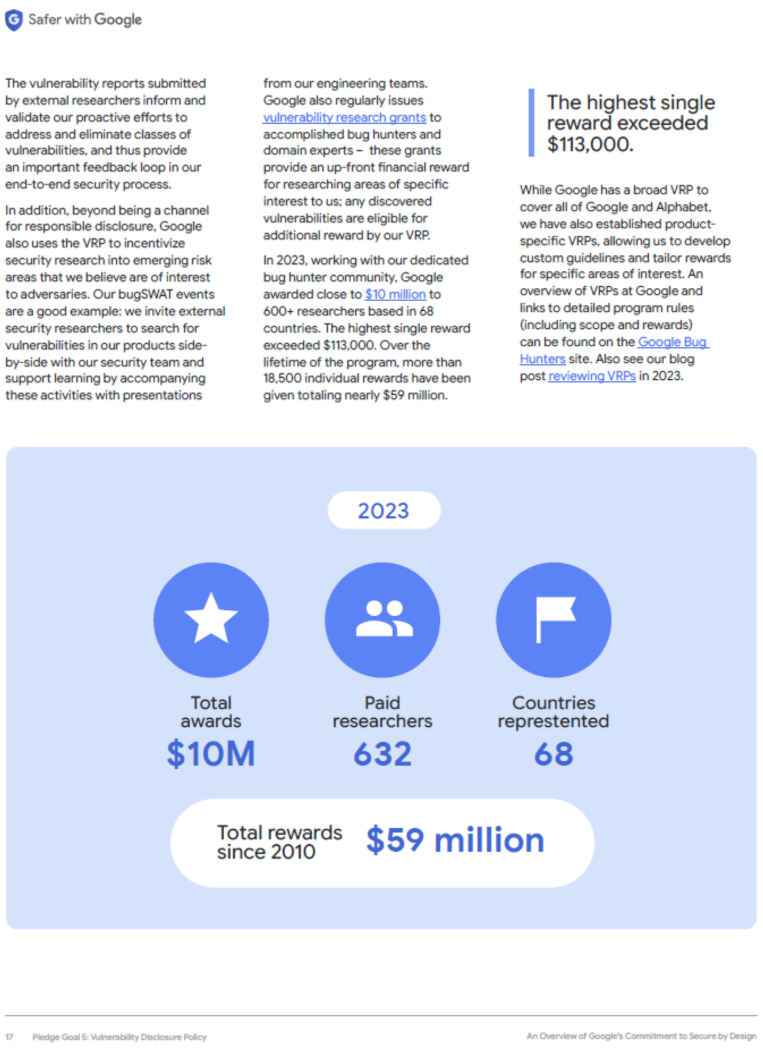
May 2023
Google First-Party Mobile App VRP announced

Google has been collaborating with external security researchers since 2004. Our reporting process encourages direct engagement, fostering a community-based approach to address security concerns.[19] Security researchers are encouraged to report issues to us that are discovered responsibly (i.e., Google discourages actions that could disrupt or harm users). From there, a panel of Google security experts reviews each vulnerability report, assessing its potential impact and the sensitivity of the affected service.

Based on this evaluation, rewards are assigned, ranging from $100 to $1 million based on the complexity and severity of the issue.

Over time, Google has evolved the program by expanding what kinds of issues qualify for a reward as well as increasing reward payments.

[19] For more information on our Bug Hunters program, see also Hacking Google Episode 004.



The vulnerability reports submitted by external researchers inform and validate our proactive efforts to address and eliminate classes of vulnerabilities, and thus provide an important feedback loop in our end-to-end security process.

In addition, beyond being a channel for responsible disclosure, Google also uses the VRP to incentivize security research into emerging risk areas that we believe are of interest to adversaries. Our bugSWAT events are a good example: we invite external security researchers to search for vulnerabilities in our products side-by-side with our security team and support learning by accompanying these activities with presentations from our engineering teams. Google also regularly issues vulnerability research grants to accomplished bug hunters and domain experts – these grants provide an up-front financial reward for researching areas of specific interest to us; any discovered vulnerabilities are eligible for additional reward by our VRP.

In 2023, working with our dedicated bug hunter community, Google awarded close to $10 million to 600+ researchers based in 68 countries. The highest single reward exceeded $113,000. Over the lifetime of the program, more than 18,500 individual rewards have been given totaling nearly $59 million.

> The highest single reward exceeded $113,000.

While Google has a broad VRP to cover all of Google and Alphabet, we have also established product-specific VRPs, allowing us to develop custom guidelines and tailor rewards for specific areas of interest. An overview of VRPs at Google and links to detailed program rules (including scope and rewards) can be found on the Google Bug Hunters site. Also see our blog post reviewing VRPs in 2023.

2023

Total awards
$10M

Paid researchers
632

Countries represtented
68

Total rewards since 2010 $59 million

Pledge Goal 6: CVEs

In 1999, the project to enumerate and share Common Vulnerabilities and Exposures (CVE) was conceived as a way to normalize disparate vendor vulnerability databases, with the purpose of simplifying the implementation of security assessment tools.[20] At the time, almost all software was still released "off the shelf" and available only by download or hard-copy (e.g., CD-ROM). Users wishing to protect themselves from security issues had to be notified that they had required actions to take. CVEs were intended to fill the knowledge gap for end users.

Over the subsequent decades, industry experts and academics have debated CVE issuance, especially as attacks and software delivery mechanisms have evolved. For example, alternatives to the CVE database were instantiated to address perceived weaknesses in the original proposal (e.g., National Vulnerability Database, the defunct Open-Source Vulnerability Database (not to be confused with OSV.dev)).

Severity scoring was conceptually introduced, most notably via the Common Vulnerability Scoring System (although there are many others).[21] Taxonomies were proposed, such as the Common Weakness Enumeration (CWE) to enable data analytics and the Common Platform Enumeration (CPE) to standardize product names. Federated CVE Numbering Authorities (CNAs) now give entities operational flexibility in issuing their own CVEs. This flexibility has introduced unresolved challenges around CVE record consistency between CNAs.

While most major software producers globally, including Google, engage in use of some or all of these schemes, there are differing views amongst experts on their return on investment, scalability, efficiency, and usefulness. For example, there is no consensus on, nor consistent use in practice of, CVEs for web-based service vulnerabilities that do not require user or customer interaction to upgrade. Known issues exist with scoring vulnerability severity, namely needing to know how a piece of technology is used in a target environment to rate the issue accordingly.[22] And some of the programs for maintaining databases, scoring mechanisms, and taxonomies are maintained on a best-effort basis.

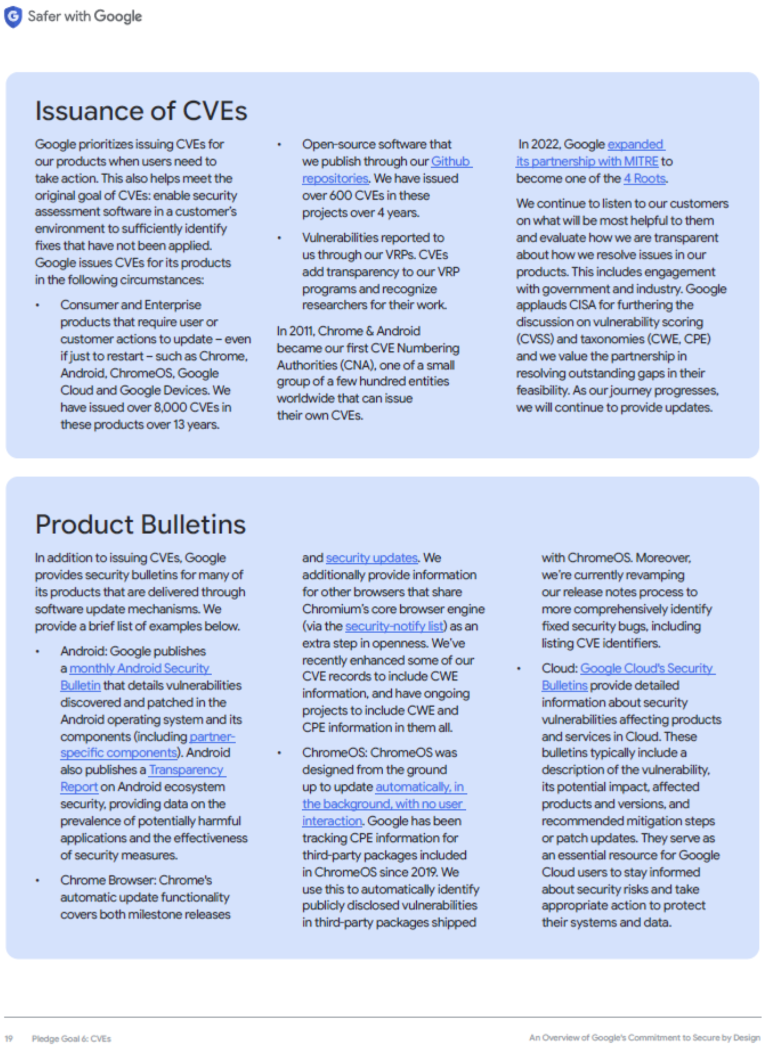
At Google we have led efforts to address these problems for open source software via the OSV Schema and OSV.dev vulnerability database. This involved working with many open source ecosystems (e.g. Python Software Foundation, Rust Secure Code Working Group) and large entities such as GitHub, Canonical, and Red Hat on adopting a common standard and distributed vulnerability database for open source software. The OSV Schema is now broadly supported across most major programming language ecosystems as well as Linux distributions, which makes OSV.dev a comprehensive source of vulnerabilities for open source software.

As part of this effort, Google also ensured that OSV maintained interoperability with CVEs. We've collaborated with CVE working groups on the CVE 5.0 standard, and aim to continue to work with them to ensure continued interoperability to help improve CVE's processes and standards.

[20] https://cve.mitre.org/docs/docs-2000/cerias.html; https://cve.mitre.org/docs/docs-2001/Development_of_CVE.html

[21] The CVSS has undergone several iterations, now on version 4: https://nvd.nist.gov/vuln-metrics/cvss. NIST is currently only "prioritizing analysis of the most significant vulnerabilities."

[22] A recent study of different vulnerability scoring systems highlights the complexities. Milousi, Konstantina et al. 2024. "Evaluating Cybersecurity Risk: A Comprehensive Comparison of Vulnerability Scoring Methodologies." In Proceedings of the 19th International Conference on Availability, Reliability and Security (ARES '24). Association for Computing Machinery, New York, NY, USA, Article 52, 1–11. https://doi.org/10.1145/3664476.3670915



Issuance of CVEs

Google prioritizes issuing CVEs for our products when users need to take action. This also helps meet the original goal of CVEs: enable security assessment software in a customer's environment to sufficiently identify fixes that have not been applied. Google issues CVEs for its products in the following circumstances:

- Consumer and Enterprise products that require user or customer actions to update – even if just to restart – such as Chrome, Android, ChromeOS, Google Cloud and Google Devices. We have issued over 8,000 CVEs in these products over 13 years.
- Open-source software that we publish through our Github repositories. We have issued over 600 CVEs in these projects over 4 years.
- Vulnerabilities reported to us through our VRPs. CVEs add transparency to our VRP programs and recognize researchers for their work.

In 2011, Chrome & Android became our first CVE Numbering Authorities (CNA), one of a small group of a few hundred entities worldwide that can issue their own CVEs.

In 2022, Google expanded its partnership with MITRE to become one of the 4 Roots.

We continue to listen to our customers on what will be most helpful to them and evaluate how we are transparent about how we resolve issues in our products. This includes engagement with government and industry. Google applauds CISA for furthering the discussion on vulnerability scoring (CVSS) and taxonomies (CWE, CPE) and we value the partnership in resolving outstanding gaps in their feasibility. As our journey progresses, we will continue to provide updates.

Product Bulletins

In addition to issuing CVEs, Google provides security bulletins for many of its products that are delivered through software update mechanisms. We provide a brief list of examples below.

- Android: Google publishes a monthly Android Security Bulletin that details vulnerabilities discovered and patched in the Android operating system and its components (including partner-specific components). Android also publishes a Transparency Report on Android ecosystem security, providing data on the prevalence of potentially harmful applications and the effectiveness of security measures.
- Chrome Browser: Chrome's automatic update functionality covers both milestone releases and security updates. We additionally provide information for other browsers that share Chromium's core browser engine (via the security-notify list) as an extra step in openness. We've recently enhanced some of our CVE records to include CWE information, and have ongoing projects to include CWE and CPE information in them all.
- ChromeOS: ChromeOS was designed from the ground up to update automatically, in the background, with no user interaction. Google has been tracking CPE information for third-party packages included in ChromeOS since 2019. We use this to automatically identify publicly disclosed vulnerabilities in third-party packages shipped with ChromeOS. Moreover, we're currently revamping our release notes process to more comprehensively identify fixed security bugs, including listing CVE identifiers.
- Cloud: Google Cloud's Security Bulletins provide detailed information about security vulnerabilities affecting products and services in Cloud. These bulletins typically include a description of the vulnerability, its potential impact, affected products and versions, and recommended mitigation steps or patch updates. They serve as an essential resource for Google Cloud users to stay informed about security risks and take appropriate action to protect their systems and data.

Pledge Goal 7: Evidence of Intrusions

Google believes it's important for customers to be able to have insight into whether cybersecurity intrusions are affecting the use of our products, and support CISA's seventh pledge goal of providing customers and users evidence of intrusions. Many of Google's products take into account how users and customers receive information about issues that may be impacting them.

Our work here is grounded in providing the right kind of insights while not overloading customers with too much irrelevant or inactionable information. We outline some examples where we've achieved this balance below, and are continuing to invest in additional insights and resources.

Google Accounts

Google provides visibility and alerting mechanisms to protect Google consumer accounts. Security Checkup provides personalized security recommendations for Google Accounts, including account recovery options, 2-step verification, removing risky access to data, and screen locks. We send Security Alerts if we detect unusual account activity on an account. And we allow users to see which devices have account access, and where they are signed in from.

Google Safe Browsing

Google Safe Browsing warns users before they visit dangerous sites and protects users from web-based threats like malware, unwanted software, social engineering, phishing, and deceptive sites. By leveraging verdicts from our detection systems, Google protects users by showing them warnings before they visit dangerous sites, or download malicious files. We've made Safe Browsing services free and publicly available for developers and other companies to use in their applications and browsers.

For users who require or want a more advanced level of security, Google offers Enhanced Safe Browsing (ESB) which provides additional AI-powered protections from the newest online threats. In Chrome, ESB users benefit from on-device and server-side models that look for signals commonly associated with malicious behavior. Furthermore, additional file protections like deep scans for suspicious files protect users from the latest malware. ESB users also get additional protection in Gmail from spam related to malicious files.

Android

Android has proactive measures and real-time monitoring and controls that alert a user to suspicious activity that could be related to potential intrusions on their device. In consumer use cases, for example, Google Play Protect (GPP) is a built-in anti-malware solution that runs on 3+ billion Google Mobile Services-enabled devices and alerts users to potential threats through a combination of on-device app scanning and cloud-based backend infrastructure. Android also has out-of-the-box detection for potential scam and phishing attacks received via Google Messages. Malicious Android apps often exhibit unusual behaviors, so we provide real-time alerting to users for apps that request Runtime Permissions, access to Android's clipboard, microphone and camera, and Background Location Access. If an app has not been used for a few months, the system protects user data by initiating a Permission Auto-Reset.

Additionally, enterprises managing a mobile phone fleet can leverage Android Enterprise capabilities to look for evidence of intrusions. Specific items include Security Audit Logs that record the device configuration and changes to it, application installations, device reboots, and other audit events. Network Event Logs and various other risk signals enable Unified Endpoint Vendors, Mobile Threat Defense Vendors, SIEM, and other security vendors to monitor network activity on the device and understand whether a device or application is running in a compromised environment.

Android also offers app developers various signals that they can leverage. For example, when an app is used on an Android device with the Google Play Store, and powered by Google Play services, the Play Integrity API provides a response that helps developers determine whether the user is interacting with a genuine, unmodified version of the app binary that Google Play recognizes. The API also provides the ability to determine whether the current user account installed or paid for their app or game on Google Play and whether the app is running on a genuine Android device powered by Google Play services (or a genuine instance of Google Play Games for PC). Developers can also choose to receive information about whether apps are running that could be used to capture the screen, display overlays, or control the device, and whether Google Play Protect is turned on and has found risky or dangerous apps installed on the device.

Google Cloud

Google Cloud operates a shared fate model which emphasizes collaboration with customers to achieve a common security and risk management goal. Google builds a foundation with built-in, always-on, and immutable controls aligned to Google's opinionated best practices, and provides actionable intelligence on security posture and risk, as well as continuous threat protection.

As a baseline for security, admin activity audit logs that capture actions that modify the configuration or metadata of resources are available for Cloud products. For example, these logs record when users create VM instances or change Identity and Access Management permissions. These logs are stored for 400 days, and users cannot configure, exclude, modify, or disable them. System event audit logs are the equivalent for Google-generated actions, and no configuration by users is required. In addition to these default audit logs, users have the option to select additional products for access to even more verbose logs, either from the Google Cloud service or from their own applications.

Cloud Logging allows for the centralization and retention of logs starting at 30 days for general logs without additional charge. Customers can additionally opt-in to keep logs for longer, up to 10 years in Cloud Logging or indefinitely in cold storage. Customers can choose the log management tool of their choice. We allow customers to use the log management tool of their choice and offer routing of logs to multiple destinations (GCS, Pub/Sub) to support other tools (Splunk, Elastic, Datadog, etc.) without Cloud Logging charges.

Google Workspace

Google offers the ability to review recent Gmail activity, including the dates, times, and IP addresses of sessions used to access the Gmail service. Users can also use Google Takeout to download "Access Log Activity," which includes multiple weeks of log information for Gmail and other Google services. In addition, Gmail users can move from this dialog to the security checkup to secure their account and device.
Gmail issues alerts to consumer users and Workspace domain administrators if a possible government-backed attack is detected.

Google Workspace domain administrators can use the audit and investigation tool and Reports API to review user and administrator activity in their organization.

Gmail issues alerts to consumer users and Workspace domain administrators if a possible government-backed attack is detected.

Google Workspace creates log events for relevant end-user actions across Google Workspace services like Gmail, Drive, Docs, and Chat, and also logs all admin actions. The default retention of these audit logs is 6 months with various audit log export capabilities.

Domain administrators can use this information to track actions performed by users and admins, and for security purposes.

For email, Google Workspace supports additional email security sandboxing, malware protection, and phishing protection, and allows admins to take actions like finding and erasing malicious emails, marking emails as spam or phishing, or sending notifications to users' inboxes.

Finally, Google Workspace domain administrators can use alert center to view notifications about potential issues within their domain, and take action (like end-user education or updates to existing policies or settings) to resolve the issues and protect their organization from security threats.

Conclusion: Building and Sustaining a Security Culture

As we outline in our book, Building Secure and Reliable Systems, security is largely an emergent property[23] of the developer ecosystem in which software is designed, implemented, and deployed. As such, it is a shared responsibility across the entire organization, not just the domain of security specialists. Everyone, from developers and Site Reliability Engineers to managers and executives, plays a role in maintaining the security and reliability of systems. Google believes that integrating security considerations throughout the entire software development lifecycle is crucial to building resilient systems.

To foster a security-first culture, Google promotes a culture of review, where changes to code and configurations undergo peer scrutiny before deployment. We leverage automation to streamline processes and minimize errors, and encourage the use of Secure by Design APIs and frameworks to guide developers toward creating inherently safer code.

Google's approach to security culture also emphasizes the importance of transparency and open communication, regularly engaging with the broader security community through initiatives like our Vulnerability Reward Programs, and encourages knowledge sharing and collaboration both internally and externally. By fostering a culture where security is everyone's responsibility and integrating security practices into the development process, Google aims to build systems that are both highly secure and reliable, ultimately providing a safer and more trustworthy experience for its users and enterprise customers. All of this is reinforced by a postmortem philosophy.

Google recognizes that creating a truly secure digital ecosystem requires a collaborative approach – one that identifies common threats and develops shared solutions that protect users across the world. We invite industry partners, policymakers, and security experts to join us in this critical endeavor. By working together, we can establish common standards, share best practices, and develop innovative solutions to combat evolving threats. We believe that through collective action – collaborating with everyone from security experts to competitors, governmental bodies, policy makers, and everyday citizens – we can build a more secure and resilient digital future for everyone.

Google supports CISA in their efforts on Secure by Design and believes that the practices outlined in this paper can help other security experts build truly defensible systems. While we have been successful in evolving and improving Google's security posture, we do not intend to rest on our laurels. We will continue to innovate and push the boundaries of what's possible in the security space.

[23] Kern, Christoph. "Developer Ecosystems for Software Safety." Communications of the ACM 67.6 (June 2024), 52-60. https://doi.org/10.1145/3651621.

Safer with Google

Contributors

Thank you to the following people, and so many others, for contributions to this paper and the work it represents.

Adam Bacchus
Adam Samet
Adam Wu
Adrian Taylor
Alex Rebert
Amy Ressler
Andres Erbsen
Andrew Eames
Andrew Pollock
Andrew Whalley
Artur Janc
Bill Creasey
Bobby Jen
Bobby Norberg
Brad Ree
Camillus Cai
Casey Sakima
Chandler Carruth
Charley Snyder
Christiaan Brand
Christoph Kern
Dave Kell
Dave Kleidermacher

David Klein
David Monsees
Deeksha Kaul
Diane Tang
Dirk Göhmann
Ed Fernandez
Elias Levy
Eugene Liderman
Hao Ke
Harini Parthasarathy
Harold Chun
Heather Adkins
Iain Mulholland
Javier Leon
Jeanette Manfra
Jeff Ma
Jeffrey Vander Stoep
Jen Engel
Jeroen Kemperman
John Gronberg
John Solomon
Jonathan Hirsch
Jonathan Li

Jonathan Rubin
Jorge Lucangeli Obes
Juan Vasquez
Kate Charlet
Keira Li
Kimberly Samra
Krzysztof Kotowicz
Lukas Weichselbaum
Mary Koes
Matthew Flegal
Matthew Riley
Max Grifka
Melanie Lombardi
Michael Groover
Mike Burr
Nicolas Lidzborski ^{SOT}
Nithan Sannappa
Oliver Chang
Pankaj Rohatgi
Parisa Tabriz
Peter Valchev
Phillip Carter
Piumi Arachchige

Rocio Vives
Roger Piqueras Jover
Ross Richendrfer
Sachin Parsewar
Salvador Mandujano
Sarah Morales
Shenaz Zack
Shuvo Chatterjee
Sławek Goryczka
Sophie Schmieg
Sri Tulasiram
Srilekha Krishnamurthy
Sriram Karra
Stefan Kölbl
Stephanie Kiel
Tatyana Bolton
Thomas Holenstein
Thyla van der Merwe
Tim Dierks
Tony Ureche
Wendy Dembowski
Will Beers
Yang Yang

Mr. GARBARINO. Thank you, Ms. Adkins.

We've been joined by Congressman Menendez.

Happy to see you here, my friend.

I now recognize Mr. Richberg for 5 minutes to summarize his opening statement.

STATEMENT OF JIM RICHBERG, HEAD OF CYBER POLICY AND GLOBAL FIELD CISO, FORTINET, INC.

Mr. RICHBERG. Thank you.

Chairman Garbarino, Ranking Member Swalwell, and distinguished Members of the subcommittee, I appreciate this opportunity to testify before you today.

My name is Jim Richberg. I serve as head of cyber policy, global field CISO at Fortinet.

Prior to my time at Fortinet, I served in the Federal Government, overseeing implementation of Government-wide cybersecurity initiatives for Presidents Bush and Obama and serving as the national intelligence manager for cyber under 2 directors of national intelligence.

Fortinet is a U.S. company that is one of the largest cybersecurity companies in the world. While we manufacture over half of the firewalls sold worldwide, our portfolio actually extends across nearly 60 different integrated security and networking solutions.

We also run an award-winning cybersecurity training institute with educational partners across the United States. We appreciate this subcommittee's focus on cyber work force efforts, including the PIVOTT Act.

We have a broad domestic footprint of over 4,000 employees in the United States and people or infrastructure in virtually every State. We recently hosted committee staff for a work force development discussion at our headquarters in Sunnyvale, California.

Ranking Member Swalwell, we appreciate you taking time to visit our facility in Union City. We have facilities across the country, including Florida, Texas, Georgia, and Illinois.

Now, I represent Fortinet in the council that serves as the IT sector's voice and partner for collaboration with CISA, and the council asked me to help lead its collaboration with CISA on Secure by Design.

Industry was already working on Secure by Design, but as a concept it gained prominence as a part of the 2023 National Cybersecurity Strategy and in subsequent CISA-led white papers. These described the potential of Secure by Design but did not constitute an actionable road map for IT manufacturers or their customers to follow.

So CISA began to work with our IT council to craft this voluntary pledge that software producers could use as a starting point. The team that worked on the pledge focused on selecting items that would be achievable by small business but also provide scope for improvement by larger and more capable companies.

Our philosophy in crafting the pledge was to agree on what to accomplish and to leave it to pledge signatories to determine how to tackle each of these goals. We were also mindful that pledge goals should yield tangible improvements to user security and produce measures of progress that could be shared publicly.

The pledge was released in May 2024, with 68 companies, including Fortinet, signing it initially. Currently, as the Chairman has noted, over 250 companies, ranging from small software developers to the largest IT firms in the world, have signed it.

Pledge signers agree to work on 7 specified goals and to report their progress within 1 year. Fortinet has been making significant progress on each of the pledge goals. I'd be happy to go into specifics in response to your questions.

I volunteered to lead industry's collaboration with CISA because of my personal belief in the value of this approach and because Fortinet has an on-going commitment to the core concepts of Secure by Design.

Radical transparency is one of those concepts. It's the idea that IT companies should disclose their product vulnerabilities, whether these are found internally or externally, and Fortinet proudly adheres to that tenet.

For too long, companies have cited each other's vulnerabilities in misleading marketing rather than acknowledging that everyone should find and mitigate vulnerabilities. We hope this pledge helps mature the sector's approach to this important issue, which is one that affects both cyber resilience and economic competitiveness.

While Secure by Design has been shown by Fortinet and other early adopters to be achievable, this approach will only succeed if it is valued by the marketplace. Unfortunately, this is not like the movie "Field of Dreams" where, if you build it, they, the customers, will automatically come. The crucial step will be in creating viable "secure by demand."

In my work with executives at major companies, I've found that few of them have heard of Secure by Design but that virtually all of them are interested in considering it as at least a possible factor in procurement. At this point, customers can likely find a supplier in most major software categories who has signed the pledge.

In my experience, letting market forces drive change is a powerful and practical approach to improving security and resilience. While Secure by Design is not a panacea, it can be a powerful lever for private-sector-led progress in cybersecurity. This concept is a work in progress, and like the process of creating the current pledge, its success will require continued public-private partnership.

I thank you for the opportunity to be part of this important hearing and look forward to today's discussion and your questions.

[The prepared statement of Mr. Richberg follows:]

PREPARED STATEMENT OF JIM RICHBERG

DECEMBER 5, 2024

Chairman Green, Ranking Member Thompson, Chairman Garbarino, Ranking Member Swalwell, and distinguished Members of the subcommittee, I appreciate the opportunity to testify before you today on "Secure by Design", which is an important but little understood tool for improving cybersecurity. My name is Jim Richberg and I serve as head of cyber policy and global field chief information security officer at Fortinet.

Fortinet[1] is a U.S. company that is one of the largest cybersecurity companies in the world. While we manufacture over half of the firewalls sold world-wide, our portfolio extends across nearly 60 different integrated cybersecurity and networking solutions and services, reflecting our commitment to innovation as information technology (IT) and cyber threats continue to evolve. In addition to our products and services, Fortinet operates a robust cybersecurity training institute[2] focused on helping to address the significant global cyber workforce and skill gaps and enabling a more digitally secure society.

Fortinet is part of numerous collaborative activities between industry and the U.S. Government, ranging from participation in the IT sector's coordinating council to collaboration on technology development through NIST's National Cybersecurity

[1] *https://www.fortinet.com/corporate/about-us/about-us.*

[2] *https://training.fortinet.com.*

Excellence Partnership[3] and coordinated cyber threat analysis and response via the Joint Cyber Defense Collaborative[4] (JCDC) run by the Cybersecurity and Infrastructure Security Agency (CISA). Reflecting the fact that cyber crime does not stop at country borders, Fortinet also participates in global initiatives such as the World Economic Forum Centre for Cybersecurity[5] and the Cyber Threat Alliance.[6]

I represent Fortinet in multiple public-private sector fora and work with governments and large enterprises across the United States and globally to address complex cyber problems ranging from Artificial Intelligence to Zero Trust. My knowledge of cybersecurity, the cyber threat landscape, and the need for building cyber resilience within organizations and nationally is based upon my 33 years of service in the U.S. Government as well as my work at Fortinet. I oversaw the implementation of the whole-of-Government Comprehensive National Cybersecurity Initiative[7] for Presidents Bush and Obama. I also served as the National Intelligence Manager for Cyber under 2 directors of national intelligence and was responsible for creating a unifying cyber strategy for the U.S. intelligence community and for setting its cyber threat priorities.

Information Technology is part of U.S. critical infrastructure, and I am honored to represent Fortinet in the Sector Coordinating Council[8] that serves as the sector's voice and partner for collaboration with CISA, which is the Sector Risk Management Agency for IT. As a Council member, I was one of the leaders in its extensive collaboration with CISA on Secure by Design and I am well-positioned to talk about this initiative both broadly and in depth.

WHAT IS SECURE BY DESIGN AND WHERE DID IT COME FROM?

Secure by Design was part of the 2023 U.S. National Cybersecurity Strategy,[9] which recognized the need for a fundamental shift in how the United States should allocate roles, responsibilities, and resources in cyber space. The Strategy noted that "We must rebalance the responsibility to defend cyber space by shifting the burden for cybersecurity away from individuals, small businesses, local governments, and infrastructure operators, and onto the organizations that are most capable and best positioned to reduce risks for all of us."[10] This meant shifting the focus of responsibility toward the producers of the IT products and services which are vital to individuals, organizations, and our critical infrastructure.

Following the release of the U.S. National Strategy, Secure by Design was described in greater depth in a White Paper[11] authored by CISA, other U.S. Government agencies, and international partners in 2023. Its guidance for IT manufacturers focused on 3 core principles:

1. "The burden of security should not fall solely on the customer. Software manufacturers should take ownership of the security outcomes of their customer's purchase and evolve their products accordingly.
2. "Embrace radical transparency and accountability. Software manufacturers should pride themselves in delivering safe and secure products, as well as differentiating themselves from the rest of the manufacturer community based on their ability to do so. This may include sharing information they learn from their customer deployments, such as the uptake of strong authentication mechanisms by default. It also includes a strong commitment to ensure vulnerability advisories and associated common vulnerability and exposure (CVE) records are complete and accurate. However, beware of the temptation to count CVEs as a negative metric, since such numbers are also a sign of a healthy code analysis and testing community.
3. "Build organizational structure and leadership to achieve these goals."[12]

The White Paper also introduced the concept of "Secure by Default", with vendors shipping products in configurations that would be effective against the most likely or prevalent threats rather than relying on users to become near-experts before they could become secure, or to follow "hardening guides" that require the customer to take specific configuration steps to operate securely. Many have cited the multi-fac-

[3] NCEP: A Mechanism for Partnering with NCCoE/NCCoE.

[4] Joint Cyber Defense Collaborative/CISA.

[5] *https://centres.weforum.org/centre-for-cybersecurity*.

[6] Home—Cyber Threat Alliance.

[7] NSPD 54: Cybersecurity Policy.

[8] IT Sector Coordinating Council—Home.

[9] National Cybersecurity Strategy/ONCD/The White House.

[10] National Cybersecurity Strategy/ONCD/The White House.

[11] Secure By Design.

[12] Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by-Design and -Default.

eted public and private-sector effort that led to dramatic improvements in motor vehicle safety[13] as proof that collective cybersecurity can be enhanced through Secure by Design manufacturer-driven action. "Secure by Default" is similar, potentially encompassing the equivalent of seat belt chimes—"noisy" and repeated reminders that would notify a user when they operate a product in a less-than-secure mode.

The Government-drafted White Paper described the potential of Secure by Design, but it did not constitute an adequate road map for either producers of software or more critically, for customers to use. Making this concept usable required sustained engagement and public-/private-sector partnership.

CRAFTING A VOLUNTARY SECURE BY DESIGN PLEDGE

To that end, in late 2023 CISA began work with the IT Sector Coordinating Council on Secure by Design with the intent of making the concept actionable in the form of a voluntary pledge[14] that producers of software could adopt and that current or potential customers could use as a guide. I co-led this process of collaboration from the industry side.

CISA had the pen but was open to industry's input on both specific content and the structure of the Pledge. While recognizing that signing the Pledge was going to represent a purely voluntary commitment, CISA was adamant that it be viewed as an "all or nothing" undertaking by signatories rather than something where they would "cherry pick" goals to work on. CISA and the industry team that worked on the Pledge focused on selecting and framing actions that could be achievable even for small businesses, but also provide room for improvement by larger and more cyber-capable companies.

Our philosophy in crafting the Pledge was to agree on goals to be pursued without prescribing any specific means for reaching them. In other words, industry and CISA worked to reach agreement on outcomes (what to accomplish) and left it to signatories to determine how to tackle accomplishing these goals. This is perhaps most relevant to the Pledge goal focused on eliminating entire classes of vulnerabilities, where both the specific outcomes and the means for implementation are likely to vary significantly by signatory and the type of vulnerability they have chosen to address.

We were mindful during Pledge development that its goals should generate measurable outcomes and measures of progress that could be shared with the public and with customers. We realized that, if the Pledge was to become widely adopted, its goals had to be both attainable and impactful. We also recognized that the Pledge approach was likely to be iterative, and the initial Pledge was envisioned as a "proof of concept" that could generate lessons learned to inform any further collaboration on a revised Pledge.

DETAILS OF THE SECURE BY DESIGN PLEDGE

By signing the Pledge, companies undertake to show measurable progress against the following goals within 1 year:[15]

1. *Multi-factor authentication (MFA).*—Demonstrate actions taken to measurably increase the use of multi-factor authentication across the manufacturer's products.
2. *Default passwords.*—Demonstrate measurable progress toward reducing default passwords across the manufacturers' products.
3. *Reducing entire classes of vulnerability.*—Demonstrate actions taken toward enabling a significant measurable reduction in the prevalence of one or more vulnerability classes across the manufacturer's products.
4. *Security patches.*—Demonstrate actions taken to measurably increase the installation of security patches by customers.
5. *Vulnerability disclosure policy.*—Publish a vulnerability disclosure policy (VDP).
6. *CVEs.*—Demonstrate transparency in vulnerability reporting.
7. *Evidence of intrusions.*—Demonstrate a measurable increase in the ability for customers to gather evidence of cybersecurity intrusions affecting the manufacturer's products.

The Pledge was designed to define a floor or minimum level of commitment in each of the areas addressed by the Goals and not to establish a performance ceiling. For example, cyber attackers often take advantage of poor identity and access management controls, so the Pledge calls on signatories to increase the use of Multi-Fac-

[13] *https://www.nhtsa.gov/how-vehicle-safety-has-improved-over-decades.*
[14] Secure by Design Pledge/CISA.
[15] Secure by Design Pledge/CISA.

tor Authentication (MFA) by customers. There are multiple ways to accomplish this goal, some of which provide security against more sophisticated attacks, but even basic MFA improves security compared to employing a user id and password alone.

The Pledge was publicly released in May 2024, with 68 companies—including Fortinet—signing it at the RSA cybersecurity conference. As of 1 December 2024, over 250 companies,[16] ranging from small software developers to some of the largest IT firms in the world, have signed this voluntary agreement.

FORTINET'S PERSPECTIVE ON THE IMPORTANCE OF THE PLEDGE

I volunteered to lead industry's collaboration with CISA both because of my personal belief in the potential value of this approach and because of Fortinet's industry leadership in many of the concepts at the core of Secure by Design. At Fortinet, we have a long-standing dedication to proactively incorporating and adhering to security best practices aligned with Government partners like CISA across our product development life cycle. As a company we believe that seeing Secure by Design precepts implemented more broadly would be beneficial to our collective security and that it is achievable by industry.

Secure coding practices and tools continue to improve with time, and Fortinet has combined these improving industry-wide capabilities along with internally-driven innovation. Our Secure Product Development Lifecycle Policy, which is based on secure-by-design and secure-by-default principles, helps ensure that security is built into each product from its inception and covers every stage of the product life cycle from initial design through to the end of product use.

EMBRACING RADICAL TRANSPARENCY

Computer code is written by humans and given the size and complexity of modern software programs, mistakes in creating or maintaining software or in user configuration of a product are virtually inevitable. The growth in computing power, new modes of connectivity, and ever-expanding malicious actor tactics, techniques, and procedures also drive the exploitability of vulnerabilities. In general, software vulnerabilities can be found by 1 of 3 sources:

1. The manufacturer of a product, who is arguably the most familiar with its functions and inner workings.
2. Customers who may encounter problems or anomalies during use, and third-party security researchers who explicitly look for potential problems. If these problems are reported to or shared with the manufacturer, they may be fixed or "patched".
3. Malicious actors who, when they find a vulnerability, exploit it rather than report it for mitigation.

Fortinet is proud that nearly 80 percent of the vulnerabilities discovered in its products in 2023 were identified by the company internally (No. 1 above) rather than found by outsiders (No. 2 and No. 3).

Radical Transparency is one of the core tenets of Secure by Design. If something matches the characteristics of a CVE, Fortinet is committed to reporting it as such rather than fixing the problem in the guise of a "performance enhancement". To improve national cyber resilience and consumer awareness, Fortinet believes that IT companies should collectively practice such "radical transparency" with respect to their disclosures of vulnerabilities, whether they are found internally or externally.

Correctly and comprehensively cataloging problems, patches, and upgrades is important. Large organizations often devote resources to verifying that a patch works as intended and to validating that it does not break something else in an organization's IT environment before they will install the update. While well-resourced organizations may have the staff and budget to perform this validation and verification process, their resources are finite. Organizations will often make the decision whether to perform validation and verification based on whether a software update is to a function that is relevant to them. If a security vulnerability is mischaracterized as a "bug fix", "performance enhancement" or functional upgrade, a company may not apply a patch without realizing that its security is affected by the underlying vulnerability that the patch addresses.[17]

As a rule, smaller organizations and individual users typically don't have a formal process or policy with regards to patching. They often fail to patch due to resource limitations or because they are not even aware of an update's existence. For these users, a vendor policy of automatically updating software will result in more widespread patching and increased security for these enterprises and users.

[16] Secure by Design Pledge Signers/CISA.

[17] How Proactive Responsible Radical Transparency Benefits Customers/Fortinet.

FORTINET'S PERFORMANCE ON THE PLEDGE

Fortinet has been making significant progress implementing the specific goals outlined in the CISA Secure by Design Pledge since signing it in May 2024. Our efforts [18] include:

- Eliminating default passwords and prompting users to create strong passwords during the product installation process.
- Implementing automatic/by default update capabilities for products typically used by small and medium-sized organizations—automatically remediating security issues (applying security patches) while allowing users to opt out if desired.
- Demonstrating transparency through reporting all Common Vulnerabilities and Exposures (CVEs) along with the accompanying Common Weakness Enumeration (CWE). This is important since CISA has observed that many organizations will report a vulnerability without noting the class (CWE) of activity it belongs to. This omission makes it difficult to use the National Vulnerability Database of CVE's for either strategic analysis (e.g., to determine which are the most prevalent classes of vulnerability) or tactically (enabling an organization to search by the classes of weakness relevant to itself).
- Publishing a machine-readable security policy and portal for our customers or third-party researchers to use in reporting any vulnerabilities they find in Fortinet products.
- Working to eradicate whole classes of vulnerability.

Fortinet is working on numerous initiatives aligned to the other Pledge objects as well, such as providing greater support to help customers using end-of-life products transition to newer supported versions.

WHAT'S NEXT? LOOKING BEYOND THE SECURE BY DESIGN PLEDGE

Secure by Design and Secure by Default have been shown by Fortinet and other early adopters to be viable for IT manufacturers to implement and to generate measurable improvements in their customers' security. However, this approach will only succeed if it is recognized and desired by the marketplace—and unfortunately this is not like the movie "Field of Dreams" where if you build it, they (customers) will automatically come. The crucial step will be in creating viable "Secure by Demand".

I speak frequently with cybersecurity and IT executives at major companies and have found that few of them are aware of Secure by Design—but that virtually all of them were interested in considering it as a possible factor in procurement decisions. A logo or symbol indicating that a manufacturer has signed the Pledge and an accompanying consumer awareness campaign could help increase overall user awareness of Secure by Design. There is a potential role for both Government and the private sector in accomplishing this.

At this point, over 250 companies representing a significant portion of the software market have signed the Pledge, and customers likely can find a supplier in most major categories of software who has signed the Pledge and made a commitment to showing what they have done to implement it. Over a dozen allied governments joined the United States in co-authoring the Secure by Design White Paper,[19] making participation in fielding products demonstrating the Secure by Design approach more attractive to companies that sell IT in multiple national markets.

Broadening the scope and application of this concept beyond IT could also help build demand, and work is under way to apply the concept to Operational Technology (OT) as well. But while the Operational Technology environment has a significant overlap with IT in terms of security problems and solutions, significant differences make a wholesale "lift and shift" of the IT-focused model impractical for OT. The ecosystem of producers and customers is different, and the product life cycle is dramatically longer, with OT systems often kept in service for 30 years or more rather than replaced every few years as in IT. Mission priorities also differ, with OT operators emphasizing safety and reliability over security.

CONCLUSION

As one who has worked on cybersecurity in both the public and private sectors, I believe that letting market forces drive broad change is a powerful and practical approach to improving our cybersecurity and digital resilience. Secure by Design is

[18] *https://www.fortinet.com/blog/industry-trends/fortinet-progress-on-its-secure-by-design-pledge-commitments.*

[19] Secure-by-Design/CISA.

not a panacea but it can be a powerful lever for private sector-led enhancement of our cybersecurity. This concept is a work in progress, and like the process of creating the current Secure by Design Pledge, its ultimate success will require continued public-private partnership. We in industry stand ready to assist the committee, and I thank you for the opportunity to be part of this important hearing. I look forward to today's discussion and I welcome your questions.

Mr. GARBARINO. Thank you, Mr. Richberg.

I now recognize Mr. Fry for 5 minutes to summarize his opening statement.

STATEMENT OF SHANE PAULSEN FRY, CHIEF TECHNOLOGY OFFICER, RUNSAFE SECURITY, INC.

Mr. FRY. Thank you, Chairman Green, Subcommittee Chairman Garbarino, Ranking Member Swalwell, and esteemed Members of the committee. I appreciate the opportunity to address you today on CISA's Secure by Design initiative.

My name is Shane Fry, and I'm the chief technology officer of RunSafe Security, having joined the company in 2018 after spending time in the U.S. Government and in commercial organizations performing advanced cyber research. I spent the majority of my career focused on devices commonly found in critical infrastructure.

Implementing the practices of Secure by Design has helped RunSafe Security improve the security and reliability our software and, thus, the security and reliability of our customers' systems, which include critical infrastructure and military weapons systems. It took us approximately 6 months to write our relatively small code base into Rust, including time to verify completeness and perform extensive testing.

Since signing the Secure by Design pledge, we've integrated SBOM generation into our builds and plan to host these SBOMs publicly alongside each of our releases. We strongly believe that companies pledging to do Secure by Design should do so as publicly and transparently as possible, and our pledge has accelerated our plans to be more public about the security posture of our software.

Secure by Design is a robust program that stands to shape development practices for decades to come. It has helped reinforce important cybersecurity concepts like software supply chain security and memory safety. It serves its role well as a North Star for software and device developers, and its importance can been seen by the large number of companies that have signed the Secure by Design pledge.

The mechanics for organizations to achieve true, complete Secure by Design, however, can take years or even decades for existing software and systems, risking the program's relevance if bridges to Secure by Design aren't encouraged.

As it pertains to critical infrastructure protection, the vision of Secure by Design meets the reality of legacy hardware, trillions of lines of code, and complex vendor supply chains. Unfortunately, our adversaries won't stop their campaigns of weaponizing our critical infrastructure to achieve their geopolitical objectives while we get our cyber house in order.

In a hearing before the Select Committee on the Chinese Communist Party in January, witnesses laid out with stark clarity that China is pre-placing cyber weapons inside our critical infrastructure in order to disrupt basic citizen services such as water, transportation, communication, and energy.

FBI Director Wray also indicated that if every cyber asset at the FBI was directed to counter China, ignoring all other threats, China's hacking forces would still outnumber the FBI assets 50 to 1.

Companies we're working with have told us it will take 8 years or more to fully implement aspects of Secure by Design. So, with 50 times our assets and 8-plus years to continue placing cyber weapons, our critical infrastructure might not be ours by the time we are Secure by Design.

One of the key but otherwise esoteric issues covered by Secure by Design is memory safety. In recent years, NSA, ONCD, Congress, and CISA have all increased visibility on the risks caused by memory safety issues.

Memory safety attacks take legitimate software and stitch pieces of them together in unauthorized ways to hijack the system. Memory safety vulnerabilities account for about 70 percent of vulnerabilities in critical infrastructure and often have the highest severity rating.

Secure by Design guides device manufacturers to rewrite all their software into a memory-safe language like Rust.

According to a former Gartner analyst, the cost of rewriting that software can be approximated, though, between $40- and $70 trillion. For many reasons, that transition to Rust is mechanically impossible within the next 5 years, leaving our infrastructure exposed to attack.

Studies undertaken by firms at the leading edge of automating code rewrites to Rust indicate that tools are only able to safely handle about 5 percent of the effort. DARPA's TRACTOR effort will hopefully improve that, but we're a few years out from real results there.

Finally, there are extensive challenges utilizing memory-safe languages in industries with safety certification requirements.

Despite the challenges we've discussed, the committee has many compelling paths forward, and CISA's investment in Secure by Design will be essential at every turn. So please allow me to present some suggestions on how industry and Government can work together to meaningfully improve the security of critical infrastructure.

First, CISA should revise Secure by Design to encourage device manufacturers to immediately implement existing commercial solutions that prevent exploitation and memory safety vulnerabilities.

Second, the U.S. Government should lead by example. All Government-developed or -required software should require compliance with Secure by Design.

Third, Congress should find ways to encourage critical infrastructure asset owners to update software in a timely manner so that Secure by Design updates are actually deployed to fielded devices.

Fourth, CISA should include critical infrastructure manufacturers in its Secure by Design pledge program. CISA's pledge explicitly excludes physical products, which ends up excluding most industrial control systems products. The results are clear: None of the major industrial control systems device manufacturers have signed the pledge.

Finally, Congress should incentivize development of safety-certified tooling for memory-safe languages.

In closing, Secure by Design has had a tremendous impact on industry, but it has a long way to go before we can collectively declare victory.

Thank you for the opportunity to testify to this esteemed subcommittee today. I look forward to answering your questions, and I appreciate your focus on this very important program.

[The prepared statement of Mr. Fry follows:]

Prepared Statement of Shane Paulsen Fry

December 5, 2024

Thank you Chairman Green, Subcommittee Chairman Garbarino, Ranking Member Swalwell, and esteemed Members of the committee. I appreciate the opportunity to address the subcommittee today on CISA's Secure by Design initiative.

My name is Shane Fry and I am the chief technology officer of RunSafe Security, having joined the company in 2018 after spending time in the U.S. Government and then commercial organizations performing advanced cyber research, both offensive and defensive in nature. I've spent the majority of my career focused in embedded device security, particularly in devices commonly found in critical infrastructure.

Implementing the practices of Secure by Design has helped RunSafe improve the security and reliability of our software, and thus the security and reliability of our customers' systems, which include critical infrastructure and military weapon systems. While we do have a secure software development process, we felt obligated as a security company to port our software to a memory-safe language so we would not be the source of an attack on customer systems and networks. It took us approximately 6 months to port our code to Rust, including time to verify correctness of the port and perform extensive testing. Since signing the Secure by Design pledge, we've integrated SBOM generation into our build processes and have plans to host those SBOMs publicly alongside each of our releases. We strongly believe that companies pledging to do Secure by Design should do so as publicly and transparently as possible, and our pledge has accelerated plans to be more public about the security posture of our software.

SECURE BY DESIGN AS A NORTH STAR

Secure by Design is a robust program, whose development with aggressive industry engagement increases the chance it shapes product and development practices for decades to come. Instead of companies playing defense on cyber, focusing on chasing every bug, Secure by Design lays out an affirmative series of practices that can decrease the overall risk of devices. It has helped reinforce important cybersecurity concepts like software supply chain security and memory safety, which we'll come back to shortly. It serves its role well as a North Star for software and device developers and its importance can be seen by the large number of companies that have signed the Secure by Design pledge.

The only challenge with a "North Star" is that you never quite reach it. The mechanics for organizations to achieve true, complete Secure by Design can take years or even decades for existing software and systems, risking the program's relevance if "Bridges to Secure by Design" aren't encouraged. The tight, well-researched recommendations decompose into thousands of complex technical decisions that take years to implement.

CRITICAL INFRASTRUCTURE PROTECTION

As it pertains to Critical Infrastructure Protection, the elegant vision of Secure by Design meets the reality of legacy hardware, legacy processors, limited system memory, trillions of lines of code, and complex vendor supply chains. Unfortunately, our adversaries won't stop their campaigns of weaponizing our critical infrastructure to achieve their geopolitical objectives while we get our "cyber house" in order. In a hearing before the Select Committee on the Chinese Community Party in January, FBI Director Wray, then-General Nakasone, Director Easterly, and Dr. Coker laid out with stark clarity that China is pre-placing cyber weapons inside our critical infrastructure, in order to disrupt basic citizen services, such as water, transportation, communications, and energy, attempting to divert the political will of the United States from defending Taiwan when China decides to use military action to coerce

Taiwan into CCP's system, perhaps between 2027 and 2030. How important will our commitment to Taiwan be if we can't provide clean water to our populace? Director Wray also indicated that if every cyber asset at the FBI was directed to counter China, ignoring all other threats, China's hacking forces would still outnumber the FBI assets 50:1. Companies we're working with in industry have told us it will take 8–15 years, or more, to fully implement aspects of Secure by Design. With 50 times our defensive assets and 8–15 years to continue placing cyber weapons, our critical infrastructure might not be "our" critical infrastructure by the time we are Secure by Design.

MEMORY SAFETY

One of the key, but otherwise-esoteric, issues brought to the forefront of cyber hygiene conversations by Secure by Design is "Memory Safety." In recent years, the National Security Agency, the Office of the National Cyber Director, Congress, and CISA have all increased visibility on the endemic risk caused by Memory Safety issues across the economy. In short, Memory Safety issues are when an attacker is able to misuse legitimate software in memory for unintended purposes, arising primarily from systems written in C and C++. By way of an analogy, a memory safety "attack" would be similar to taking the letters, words, and spaces from Little Red Riding Hood and creating a ransom note using those same letters in a different order. Memory Safety attacks take legitimate software and stitch the pieces of the software together in unauthorized ways to hijack the system. As highlighted by the NSA, ONCD, CISA, Microsoft, and many others, memory safety vulnerabilities account for about 70 percent of the vulnerabilities in C and C++ software. Additionally, according to research by Dr. Laurie Williams at North Carolina State University, this class of vulnerabilities has a consistently higher vulnerability rating than every other class of vulnerabilities and takes twice as long to fix.

Secure by Design guides critical infrastructure device manufacturers to rewrite all of their C and C++ software into a memory-safe language like Rust. For a litany of reasons, that transition to Rust is mechanically impossible within the next 5 years, leaving our infrastructure exposed to attack. No combination of money, people, or technology exist to achieve that. According to former Gartner analyst Brad LaPorte, now at High Tide Advisors, the cost of rewriting the software can be approximated at between $40 and $70 trillion, based on a comparison to the Y2K problem. There are not enough developers to write or maintain that much Rust. Additionally, the salaries for existing Rust developers tend to be in the top quartile of developer salaries, causing any rewrites to draw on the most constrained and expensive resources. Even if one device manufacturer chooses to write all of their code in Rust, the supporting dependencies in the operating system might not be present in a memory-safe language. Even recent studies undertaken by firms at the leading edge of automating code-rewrites from C to Rust indicate that humans are still needed for 95 percent of the effort, with tools only able to handle 5 percent of the effort. Finally, there are extensive challenges utilizing memory-safe languages in certain critical infrastructure industries where software needs to meet safety certification requirements, for example DO–178 in aviation and ISO 26262 in automotive.

PROPOSED SOLUTIONS

Despite the challenges we've discussed, the committee has many compelling paths forward and CISA's investment in Secure by Design will be essential at each turn. So please allow me to present some suggestions on how industry and Government can work together to meaningfully improve the security of critical infrastructure:

1. CISA should modify Secure by Design to incorporate memory protections into existing devices today by encouraging device manufacturers to implement existing commercial solutions that prevent exploitation of devastating memory safety vulnerabilities even without rewriting a single line of code.
2. The U.S. Government should lead by example: U.S. Government-developed software should adopt software memory protections today and all funded acquisitions of devices or software should mandate compliance with Secure by Design.
3. Congress should find ways to encourage critical infrastructure asset owners to update software in a timely manner. Assuming every device manufacturer adopts Secure by Design and has secure releases available tomorrow, a huge hole still exists in critical infrastructure: a software update that is secure by default but is never deployed to fielded assets does not make critical infrastructure any more secure than it is today. None of CISA's current efforts, Secure by Design, Secure by Default, or Secure by Demand address this problem.

4. CISA should include critical infrastructure manufacturers in its Secure by Design Pledge program. For some unexplainable reason, CISA's pledge explicitly excludes physical products, which ends up excluding most critical infrastructure products. The results are clear: none of the major critical infrastructure manufacturers have signed the pledge.

5. Congress should incentivize development of safety certified tooling for DO–178/DO–330 and ISO 26262 certification and ISA 62443.

CLOSING

Secure by Design has already had a tremendous impact on industry, but it has a long way to go before we can collectively declare victory. Thank you for the opportunity to testify to this esteemed subcommittee today. I look forward to answering your questions and I appreciate your focus on this very important program.

Mr. GARBARINO. Thank you, Mr. Fry.

I recognize Dr. Mukkamala for 5 minutes to summarize his opening statement.

STATEMENT OF SRINIVAS MUKKAMALA, BOARD OF REGENTS, NEW MEXICO TECH; EL PASO ELECTRIC

Mr. MUKKAMALA. Thank you, Chairman Garbarino, for having me here, Member Swalwell, and the rest of the committee Members.

So my name is Srinivas Mukkamala. So I have a really unique representation, being on the Board of Regents of New Mexico Tech, which was just featured in the RAND report last week on kinetic warfare and how the United States will be up for a rude shock. That work is actually being done south, on the Southern Border of the United States, called Playas, where we look at every single communication system and look at, if there is vulnerable software, how can that take down our men and women on the front lines. This was just published last week.

I also represent a utility, one of the largest utilities in the country, which also owns the largest nuclear power plant, and a border, supports 3 bases, and I'm an independent board member there.

I also represent Cowbell Cyber, which is in the Congressman's district, which insures small and medium businesses in an event, if there is an unfortunate thing, how do you really defend yourself?

So a very interesting perspective from 3 different walks of life—training the future cyber citizens; really looking at how do you power AI, generating power, the livelihood; and the third one is, if you're at an incident, how do you recover from that?

So I was a fortunate recipient of the Congressional support for getting my degree in AI and cybersecurity in 2000. A lot of people talk about cybersecurity today; very few of us actually were trained in cyber, in AI, 25 years ago. We didn't learn on the job. We didn't learn it by choice. We actually went to school for that. That gives us a very good understanding about the fundamentals of what's working and what's not.

So what I want to focus on is a class in 2001 which was paramount, software integrity class that was taught in major universities. Zero-defect software was the theme, and written by Allan Stavely from New Mexico Tech. We cannot have software with errors. I'm talking 25 years ago. The case study which we all studied was the Therac–25. It's a risk condition that killed people with those issues.

Today, 25 years later, we're talking memory-safe, we're talking risk conditions, and it is one of the examples CISA talks about you can't have in your court—25 years later.

In 2005, a program called Build In Security, by DHS, with Carnegie Mellon, was introduced. Again, a voluntary program. Every vendor said, we will follow this, we will have built-in security. Twenty years later, we're still talking Secure by Design.

I think we have a fundamental challenge, and we are up for a rude shock. There are two alarming scenarios I want to bring to the committee's attention.

The first one is a multi-trillion-dollar tech debt program. It's a real problem. We talk about financial debt; we talk about printing money. We have a real tech debt problem.

The second one is, we have $1.4 trillion worth of software installed on systems running critical infrastructure around the world. This is what's giving the adversaries an asymmetric advantage. It is not their sophistication. Yes, they're sophisticated, but it's really the software errors that's giving them the advantage. Not us being resilient and not being able to respond on time is allowing the so-called Chinese actors, North Korean actors, Korean actors—you name the actor—to own our systems and cause havoc.

One of the questions we should ask for ourselves: When we have a system of truths like National Software Reference Library, we have the national vulnerability software library, NVD, why don't we have a national legacy software library?

Because that brings real transparency. As a consumer, I know that I'm using a legacy software. Why are we not developing that nationally and educating the consumers? That will force the vendors to get away from legacy software. We expect the consumer to know what they're buying, but unfortunately we might not.

There are 3 things I want to bring to the committee's attention.

We need to have transparency, and lack of accountability is not helping. That needs to be enforced, and that needs to be really brought to the forefront.

The second one is, we need to define classes of vulnerabilities. We keep talking about different rankings, "top 25 most dangerous common weaknesses." That ranking changes every other year. There is a legacy ranking, there's a current ranking, and when you start looking at the future rankings for AI, which we all are talking about, it's a very different ranking. So what am I going to hold you accountable for? What is your guidance? What do you really want us to do?

The third one I want to really talk about is, software safety is not a choice. It is not a design thing. I mean, design is important, but you cannot—I mean, you won't even buy a stroller without a safety symbol on it. Why am I using software without a safety symbol on that and letting critical infrastructure run? We regulate medical devices, we regulate utilities, we regulate every single thing around us. Why not software?

I think it's paramount, it's about time to make sure there is assurance on the software that's being put on consumers, that runs national security systems and critical infrastructure, so we all can be assured and be confident that we are actually running a reliable software and we are not in danger.

With that, thank you for this opportunity. I'm happy to answer any questions.

[The prepared statement of Mr. Mukkamala follows:]

PREPARED STATEMENT OF SRINIVAS MUKKAMALA

THURSDAY, DECEMBER 5, 2024

Software errors can be a significant reason for safety issues, as malfunctions caused by bugs in code can lead to dangerous situations in systems that control critical functions like medical devices, transportation systems, or industrial machinery, potentially causing harm to users or the environment if not properly addressed.

A good example and a case study in most U.S. universities software integrity course curriculum is The Therac–25.

The Therac–25 is a computer-controlled radiation therapy machine produced by Atomic Energy of Canada Limited (AECL) in 1982. It was involved in at least 6 accidents between 1985 and 1987, in which some patients were given massive overdoses of radiation. Because of concurrent programming errors (also known as race conditions), it sometimes gave its patients radiation doses that were hundreds of times greater than normal, resulting in death or serious injury. These accidents highlighted the dangers of software control of safety-critical systems.

We have 2 alarming scenarios at hand as I testify on Dec 5, 2024:

- A report published by *Forbes:* A Trillion-Dollar Global Tech Problem, a recent study examined the increase in tech debt from 2012 to 2023 across industries and regions reveals global tech debt has nearly doubled over this time frame, increasing by around $6 trillion.
  - In the United States, 3 sectors are responsible for 64 percent of the estimated $2.2 trillion rise in tech debt: banking and investment services; communications, media, and services; and Government.
- $1.14 Trillion to Keep the Lights on: Legacy's Drag on Productivity published by Mechanical Orchard. January 23, 2023.

Legacy systems run code or rely on libraries that might contain known security vulnerabilities with no way to patch these. Dated, insecure code increases the attack surface for a business.

In its 2019 study of several critical Federal Government systems, GAO noted that several of the legacy systems were operating with known security vulnerabilities and unsupported hardware and software.

What is alarming is the lack of transparency and a catalog of legacy systems and software serving critical infrastructure. We have several initiatives to catalog know software (NSRL—The National Software Reference Library) and known vulnerabilities (NVD—National Vulnerability Database). An initiative to catalog legacy software and publish known weakness and vulnerabilities will allow entities to better understand the risk posed by legacy software.

KEY POINT 1: TRANSPARENCY AND LACK OF ACCOUNTABILITY

Initiatives like "Secure by Design" and Build Security In (a 2005 initiative) bring the required awareness that is needed to address the problem at hand.

"Secure by Design" is a voluntary pledge focused on enterprise software products and services. By participating in the pledge, software manufacturers are pledging to make a good-faith effort to demonstrate measurable progress toward the following areas.

We can't afford good faith in safety. Recent attacks have demonstrated the impact on critical infrastructure from Water Utilities to Food Processing units.

What's needed is radical transparency on the pledge, a catalog of software by the vendor what is covered and what is not. A clear time line to demonstrate progress in securing legacy and vulnerable software that is been neglected for years.

How Food and Drug Administration (FDA) holds drug and product manufacturers automatically liable for any harm caused by their product. Congress can also establish a software liability regime for software manufacturers.

KEY POINT 2: DEFINING CLASSES OF VULNERABILITY AND DEVELOPING A TAXONOMY

One of the goals in the pledge is to reduce entire classes of vulnerability. Within 1 year of signing the pledge, it will demonstrate a significant reduction in the prevalence of 1 or more vulnerability classes across the manufacturer's products.

Without a proper definition and a prescriptive list of Common Weaknesses and Vulnerabilities that needs to be reduced or eliminated there is room for interpretation and not yield desired results.

Based on our research and analysis of 25 Most Dangerous Software Weaknesses list (CWE™ Top 25) is the positioning of memory buffer operations. While MITRE ranks this at No. 20, it consistently appears as the top target for both threat groups and ransomware operators.

We also observed significant evolution in the threat landscape, particularly with the emergence of AI/ML systems.

Organizations must adapt their security priorities to address these changes, with special attention to emerging AI/ML-specific vulnerabilities that may not yet be reflected in standardized rankings.

KEY POINT 3: A SAFETY SEAL FOR SOFTWARE

Software runs multiple critical infrastructure sectors. What is rapidly changing is the digital transformation and autonomous nature of how these systems operate today. There are several sectors that follow rigorous quality tests and checks before they are deployed in production. Congress can establish a safety framework for software industry as well.

Mr. GARBARINO. Thank you, Dr. Mukkamala.

Members will be recognized in order of seniority for their 5 minutes of questioning. An additional round of questioning may be called after all Members have been recognized.

I now recognize Mr. Ezell from Mississippi for his 5 minutes of questions.

Mr. EZELL. Thank you, Mr. Chairman.

Everybody's been impacted in one way or another by these cyber attacks on CrowdStrike, Microsoft, and several others. So I'm pleased that we're continuing to have a discussion on this very important matter.

The Secure by Design pledge is a good step toward incentivizing businesses to create more secure products.

I want to be clear that, while I support efforts such as these, I'm always concerned by efforts to codify or mandate these requirements for businesses. Mandates are often duplicative, costly, and burdensome in time and resources.

We have seen over 250 companies, including our industry representative witnesses here today, already sign this pledge to improve and strengthen their cybersecurity.

I want to kind-of just go down the line with all of you today. I'd like to thank each and every one of you for your commitment, for being here today. I'm sure you could be plenty of other places, so thank you very much.

I'd like to discuss a little bit more which of the 7 pillars has been the hardest to adopt and why.

I'll start with you, Ms. Adkins, and just kind-of go down the line.

Ms. ADKINS. Well, I would say, there is complexity in all 7, but I would probably rank classes of vulnerabilities as one of the most difficult.

The reason being is that, to really fix this problem in its kind of purest form, you have to change the way developers work. In the work force—you know, at a company, you have some control over that. But we rely on third-party software, we rely on open-source software, where we don't have any control over how that software is developed as well. So the kind-of full list of materials that go into the software is hard.

So we have had to spend a lot of time really innovating in that space to make sure that the way we write code is safe. Now, with generative AI, we've got this great new tool, actually, that we think, you know, after, you know, 3 to 5 years of research we're going to have an even better tool.

Mr. EZELL. OK.

Ms. ADKINS. Yes.

Mr. EZELL. Would anybody else like to comment about that?

Mr. RICHBERG. So I would indisputably say No. 3, on tackling entire classes of vulnerabilities. But I bring guilty knowledge as someone who literally helped craft the things.

Some of them are very binary, one and done. Do you have a policy on vulnerability disclosure that lets people test you? You write it; you don't.

This one was intended as the stretch goal for companies like Fortinet and Google, where tackling by the things we've talked about—memory-safe programming languages, addressing SQL injection—that one was intended as something where there are a large number of classes of vulnerability. You can succeed in tackling them serially, but even for big companies, it's going to take us a long time to knock off all of those.

Mr. EZELL. Thank you.

Anybody else?

Mr. FRY. So I would agree; I think tackling all classes of memory vulnerabilities is probably the hardest. The number of developers out there that can write code in those memory-safe languages is very limited. They are the most expensive engineers you can pay today, and that's really challenging.

Now, there are some classes that are easier to solve than others, and, you know, there's definitely great frameworks for that.

The other thing that I see in talking to a lot of industrial control systems manufacturers is not the generation of software build materials but their willingness to share them. So they treat them almost more than the intellectual property of their source code. That, I think, is a huge challenge for some of these companies to overcome, is accepting that part. But they're going to be way behind on the memory safety conversion as well and getting that whole class of vulnerabilities covered.

Mr. EZELL. Thank you.

Doctor.

Mr. MUKKAMALA. So I'd like to add an important aspect. I agree with Ms. Adkins on that is the hardest problem, for 3 reasons.

There's a human involved. Most of our developers today are not trained in software security. That is a real problem. They lack training. The other thing that's also causing a real issue is, majority of the software is actually built offshore.

I can give an example for India. Indian universities do not train their students, not have a curriculum on software security. I was trained in India. Still today, I was looking at a curriculum from the top Indian Institute of Technology, IIT, which majority of the CEOs in this country are from those schools, their undergraduate. They're not trained in software security. You have a critical gap. That's No. 1.

No. 2, we have legacy software. We might not even have the source code for us to go back and look at what are the weaknesses and what are the vulnerabilities. You're looking at compiled code. You have limited visibility into that. Even if you find a vulnerability, people are very concerned, because it's not well-documented, you're going to break something, so you'd rather leave it the way it is.

The third most important thing, which we are not talking about—Ms. Adkins talked about AI will really help us going forward. At the same time, you'll also have a lot of machine-generated libraries, machine-generated code. What we haven't seen is, is it good, is it bad, or will it create a new class of weaknesses and vulnerabilities that we'll all have to learn from and live with?

So those are my 3 key points.

Mr. EZELL. Uh-huh.

Thank you, Mr. Chairman. I yield back.

Mr. GARBARINO. The gentleman yields back.

I now recognize the gentleman from New Jersey, Mr. Menendez, for 5 minutes of questions.

Mr. MENENDEZ. Mr. Chairman, Mr. Ranking Member, thank you for convening today's hearing.

Cybersecurity is no longer just a technical issue; it's a matter of public safety and trust.

Across New Jersey, institutions have suffered devastating ransomware attacks that threaten essential services and public confidence. Just last week, in my district, Hoboken City Hall suffered a significant ransomware attack, paralyzing vital municipal services and underscoring how vulnerable public infrastructure can be.

This incident also echoes previous attacks on educational institutions, such as Stevens Institute of Technology in 2019 and, more recently, New Jersey City University, highlighting a worrying trend. Ransomware operators are increasingly focused on exploiting the limited cybersecurity resources of local governments and schools.

These incidents serve as more than just isolated disruptions; they represent a growing threat to public safety and economic stability. This reality demands a proactive, coordinated response from industry and Government alike, rooted in principles like those found in CISA's Secure by Design initiative, which aims to shift cybersecurity responsibility from consumers to technology producers.

Today, I look forward to our focus being on understanding how we can move beyond reactive security measures; instead, more toward a proactive framework that builds resilience into our systems from the ground up.

Mr. Mukkamala, you and I agree that vulnerabilities in software can have far-reaching consequences, especially when it comes to critical infrastructure. In your testimony, you discuss the importance of making Secure by Design by a fundamental part of software development to prevent critical vulnerabilities.

If the next administration fails to build upon this initiative, what are the immediate and long-term consequences we could face, particularly regarding cyber attacks on critical infrastructure?

Mr. MUKKAMALA. So, Member, the most important thing for the next administration is to really hold software vendors accountable.

Right now, we are expecting the consumer to be resilient. Majority of the consumers—you touched on educational institutions—K to 20, they don't have the resources. You're talking about utilities.

We're talking about digital transformation, automation. There is no security guy sitting in a utility. At the best, you get 2 or 3 people. But you're talking about livelihoods of hundreds and thousands of people. You've seen American Water just got impacted by ransomware.

When you start looking at, how many security folks do I have that are trained in cybersecurity, who understand software—not systems; software—it won't even be a handful of people. We have a real problem.

That's why it's very important for the new administration to, No. 1, not encourage vulnerable software in the Federal Government. It starts there. The second is, also hold software vendors accountable if there is an error. There should be some sort of a liability because of fewer errors.

Mr. MENENDEZ. Yeah. I appreciate that.

Recent cyber incidents like the ransomware attack on Hoboken City Hall that I had mentioned earlier underscore the vulnerabilities municipalities face. This attack, which occurred last week, forced city hall to close and suspend on-line services. IT teams isolated the infected computer to prevent further damage, and essential services like the municipal court had to be relocated temporarily. Investigations are still under way to determine the extent of the cyber attack.

My question to you is, how do you see the principles of Secure by Design reducing the burden on under-resourced entities like local governments?

Mr. MUKKAMALA. So, first, there's already software running that's vulnerable. I don't think we will fix an attack right away. That's a very important thing.

For the future part, we need to make sure the software that's been downloaded is secure while we look back and look at what systems are vulnerable so we can avoid these attacks.

From the grant we have today for the State, local, and education on—there's actually a grant from CISA to support these local communities. The future administration should continue to support that. We cannot take away funding from the little money they have to secure the under-resourced organizations. We can continue to support that.

At the same time, we need to do continuous diagnostics. I know CDM is not a famous thing in the Federal Government, but if you don't diagnose, if you don't detect faster, you can't remediate. The most important thing is, we need to continue to detect, continue to prioritize, and continue to remediate. That's what we should be focusing on to avoid future attacks.

Mr. MENENDEZ. I appreciate that.

I'll yield back.

Mr. GARBARINO. The gentleman yields back.

I now recognize myself for 5 minutes of questions.

Ms. Adkins, you mentioned in your answering questions to Mr. Ezell that one of the things we have to do is change the way the developers work, you know. You're deputy chair of the Cyber Safety Review Board, so you have a unique understanding of the importance of public and partnerships and working with the private sector.

You briefly touched on it, again, in your answer to Mr. Ezell about the 7 pillars. There's issues, you think, with all of them, or there could be issues with all of them. Could you go into more detail?

Ms. ADKINS. I would say, I wouldn't characterize them as issues; I'd characterize them as complexities.

So, for example, when we went to implement multifactor authentication for our infrastructure and our users, many of the usable solutions didn't exist. Actually, users reject unusable solutions. So you have to go back to the drawing board and reinvent the way things work. That's a complexity for multifactor authentication.

When we're looking at some of the others that are in there, I think about if you, for example, want to start a vulnerability disclosure program but you haven't improved your software quality, what you're going to immediately get is thousands and thousands of reports that you already knew and is actually not that valuable to you.

So there's a journey on each one of these steps that everyone has to walk through.

Mr. GARBARINO. OK.

You know, you brought up multifactor authentication, and, you know, we know it's not all created equal, and there's threat actors that actually have been able to find a way around some of the multifactor authentications.

What could be—either Ms. Adkins or Mr. Richberg, what could be done with the 7 pillars or what could be done with that when we're talking about Secure by Design?

Mr. RICHBERG. So we set the 7 pillars—the 7 portions up to be a floor and not a ceiling, and multifactor authentication was one of those.

To your point, we recognized and there was discussion, should we specify phishing-resistant multifactor authentication, something like your phone that's cryptographically bound to you, not a text or an email that can be intercepted? But we said, recognize, we're doing this not only for the big companies but for the small start-ups. That's a high bar for them to clear. Anything is better than a user ID or password, so let's let them start with something.

Let's also recognize that this pledge is likely to be serial. We'll learn from this, and then we might have—because this is a voluntary pledge—a 2.0. We certainly talked about there's nuance in multifactor authentication.

Mr. GARBARINO. But if we're going to have a floor, shouldn't—and when we're talking about Secure by Design, shouldn't the floor be secure?

I mean, if it's not—I mean, how do we—and I get the complexities with the start-ups, but we still want them selling a secure product if they're working on this, correct?

Mr. RICHBERG. But for the things that the pledge is measuring, yes, we agreed these would all represent progress. Any form of multifactor authentication is better than single-factor authentication.

Mr. GARBARINO. I agree with you.

Mr. RICHBERG. Now, there can be more nuanced ones. We recognize, because those are commercially available, most companies would jump to that.

But we didn't want to produce a pledge that prospective signatories would look at it and say, some of these were too hard. Because this pledge was envisioned as all-or-nothing. It's not mandatory that you make progress on them, but we and CISA didn't want companies to cherry-pick, "I'm going to sign the pledge because one of these things I can do."

Mr. GARBARINO. Ms. Adkins, you had a——

Ms. ADKINS. Yes, I wanted to jump in here too.

You know, the FIDO Alliance, which is the industry coalition looking at FIDO protocols—so things like security keys, passkeys—understand this is a transition time line. But we are now at a place where passkeys are actually the most usable solution, and they are far more secure than things like SMS-based MFA. It's time to push everyone there, deprecate SMS—at least here in the United States.

Mr. GARBARINO. That was my next follow-up. I was going to ask you about passkeys, and you jumped to it before I even could.

Mr. Fry or Dr. Mukkamala, is anything you want to add to this discussion? I don't want to—I see you've been nodding, so I'm not sure if there was something you wanted to add.

Mr. MUKKAMALA. No, I'm——[off-mike], Mr. Chair.

Mr. GARBARINO. OK.

Mr. Fry, you're good? OK.

OK. So now I wanted to—Mr. Richberg, I—CISA released the Secure by Design guidance for the IT community. Your expertise is in OT.

Does the IT guidance work for OT? If it doesn't, why, and what might be some foundational elements of OT guidance that should be included?

Mr. RICHBERG. The short answer, because I know I'm short on time, is it doesn't——

Mr. GARBARINO. No, no, you can keep going. I'm the Chair.

Mr. RICHBERG [continuing]. OK—it doesn't work for OT. They share some complexities in terms of the way you think about security, but it is a much different time line, it's a different crowd. They tried grafting the pledge to the OT environment. It doesn't work.

You've got the companies, the handful of companies, that make the core chips for ICS and SCADA. You've got the larger number of companies that actually make the operational technology for specific industries. What you use for making cars is different than power plants. Then you've got the companies that buy it and customize it. They don't run it off the shelf. It's a different ecosystem.

We turn over IT in 3- and 4-year cycles. OT lasts for 30 years. So how do we implement Secure by Design in something they may not want to buy for 15 years? It's a different ecosystem.

The first version of the pledge looked like lift-and-shift, did not work; it's back to the drawing board. Full disclosure: We had to do that 5 or 6 times on the IT pledge with CISA.

Mr. GARBARINO. It sounds like OT might—you can't even do Secure by Design on some of these because of—well, let's go to Mr. Swalwell first, and then we're going to do a second round of questions.

I yield back, and I now recognize the Ranking Member for 5 minutes of questions.

Mr. SWALWELL. Thank you.

This is a distinct, informed panel that we have, and I'd like to start by just asking for your take and wisdom on the most recent FBI warning regarding the use of Android or iPhone and essentially recommending that Americans, in their text messaging, move to more encrypted applications.

I would just start with you, Ms. Adkins. I mean, it's quite alarming from a just, you know, data privacy, potential critical infrastructure for those who work in that space who use Apple or Android. Like, what can you say to that warning, and what should Americans know?

Ms. ADKINS. That warning doesn't surprise me at all. It echoes advice that the security industry has have been giving for a very long time. We understand that strong encryption is absolutely necessary for protecting information, whether it's in enterprise systems flowing over the internet, cell networks, et cetera.

What we did in Android—I can't speak to Apple's ecosystem, but what we did in the Android a little while back is to start to move away from SMS for texting into the RCS protocol. This works a little higher up the stack, and we can provide transit encryption that would protect you from the particular threat you're referencing.

Mr. SWALWELL. Now, is it correct, though, that—I believe this is so with iPhone—where, if you do not back your iMessages up on the cloud, that it's more protected than if you do, because if your Apple ID is hacked, then you can go directly into the messages, whereas——

Ms. ADKINS. Yes.

Mr. SWALWELL [continuing]. You would only need the—you would have to actually get the device——

Ms. ADKINS. Yes.

Mr. SWALWELL [continuing]. To get the——

Ms. ADKINS. So what you're talking about is one layer up in the protocol sandwich.

Mr. SWALWELL. Sure.

Ms. ADKINS. But RCS provides—is a replacement, essentially, for SMS.

Then on top of that, in Android we provide a comparable feature in Messages. So, if you're on an Android phone and you're messaging someone on an Android phone, at the most top layer that is encrypted end-to-end.

Mr. SWALWELL. How about an iPhone and an Android phone?

Ms. ADKINS. So the interoperability at that layer is something that we would really like the industry to do. It doesn't exist today.

Mr. SWALWELL. Yes.

Ms. ADKINS. But the industry group that works on RCS—this is the GSMA group—took up in September that they're going to look at end-to-end encryption which would be interoperable between all the systems.

But we're huge advocates of strong encryption to protect Americans in this situation.

Mr. SWALWELL. Great.

Would anyone else like to speak to this most recent warning?

Mr. RICHBERG. I think I would talk about it in a little more abstract fashion, in the sense that I agree with what Ms. Adkins is saying; industry groups, industry interoperability will solve it.

Asking individuals to download a third-party app to secure themselves continues to perpetuate this idea that you are—yes, you are responsible for your own security, but you shouldn't have to be the executor of it. That's what the big—that's the crux of Secure by Design: We should do that, we in industry.

Mr. SWALWELL. Right. Thank you.

Mr. Fry.

Mr. FRY. Yes, I think it's a great discussion point. One of the things, taking it maybe a step further, is not just end-users but, as you talk about, people that are deploying software and systems that maybe aren't you and I but, you know, IT, ISPs, and, you know, telco providers, they need that Secure by Design as well. They're not going to be experts in a Fortinet switch or an Android device. They're an expert in——

Mr. SWALWELL. Right.

Mr. FRY [continuing]. Sending phone messages and calls across the country.

So, you know, Secure by Design really has a great opportunity to impact that, and, by extension, you and I are protected from that as well.

But we've got to really look at what's out there today as well as what we're going to put out 5 years from now, and make sure that we're not just looking at the future but what can we do for devices that are in data centers and——

Mr. SWALWELL. Right.

Mr. FRY [continuing]. Server rooms across the country today.

Mr. SWALWELL. If, like, say, a Chinese Government actor or a criminal-gang actor was able to access, you know, millions of Americans' content, using AI you could you piece together information about that individual to access, you know, many of, you know, their most secure and protected possessions, from bank records, health records, et cetera. Is that right?

Mr. FRY. Absolutely.

Mr. SWALWELL. Dr. Mukkamala.

Mr. MUKKAMALA. The warning is too little too late.

I'll say this simple example. Folks in the intelligence community have been using Signal for a long time. There's a reason for that. This warning should have come almost 5, 10 years ago. We have known for a long time telecom infrastructure was susceptible to attacks. We have known this right after 9/11.

When we said, let's go get every communication, put a tap on so we can see communications back and forth, what does it really mean? You can go look at communications. We have known this for 21 years, and we should've paid attention to that.

We should've created secure protocols from a communications standpoint. What I'm afraid is, when you start looking at sensitive devices communicating with each other, we still don't have that. We are focused on consumer-grade. At the same time, there is so much back-end crossing that goes on in infrastructure all on clear text.

Mr. SWALWELL. Right.

Mr. MUKKAMALA. I think that's the next real ticking time bomb, for an adversary to intercept operational communications that will take down a power plant, that will take down a water facility, that will take down automobiles, which are running autonomous today. I think that's where we need to be really paying attention to, on securing communication channels.

Mr. SWALWELL. Thank you. Yield back.

Mr. GARBARINO. The gentleman yields back.

We'll now start our second round of questions. I know Ms. Lee is on her way.

Mr. Menendez, do you have—no? OK.

I recognize myself for my second round of questions.

Let's go back to the OT conversation we were having. Mr. Richberg, you were about to say something. I know Mr. Fry wanted to jump in. So let's get back at it.

Mr. RICHBERG. So I think it is going to be a soluble problem for OT, but I think, frankly, they rushed it. They needed to try to get something done and they thought they could port it. The initial version is, frankly, I don't think going to be viable and it will be back to the drawing board.

It's very much—we're at the point I think of whiteboarding. What exactly is it going to look like? Because you have different players in the ecosystem. You have different priorities.

For IT, quite often you can say security can be as important as anything else. We know for OT it's going to be safety, reliability, then maybe efficiency or performance, and then security is going to be No. 4.

So it is going to be something where the concept applies, but I think because the values, the players, and the time lines, and, frankly, constraints are different, we're going to have to come at it differently.

But it's going to be critically important, because I know this subcommittee's jurisdiction includes critical infrastructure. You've got these small players in the infrastructure, rural electric co-ops, small water utilities, who the same guy who cuts the grass and paints the building keeps the IT dusted. If it doesn't do its own security, there is no security. That's the reality where any level of Secure by Design for OT will be meaningful.

Mr. GARBARINO. Mr. Fry.

Mr. FRY. Yes. So the additional clarification that I would bring is that the companies that we talk to in industrial control systems, some of the top manufacturers, they're actively trying to figure out how they can be Secure by Design.

So while it may not have been originally designed for OT networks and OT systems and devices, there's a lot of communication happening in those companies to figure out how can we achieve this.

Now, interestingly, a lot of that was just discussion. How can we put an industry panel together? How can we comply?

Since the EU Cyber Resiliency Act has come into effect there's been actual motion of assigning engineers to doing work to become compliant with the Cyber Resiliency Act.

So that gives me a lot of promise that the United States will benefit from that and where I think device manufacturers for OT systems will actually strive to become Secure by Design, because there's so much overlap in the Cyber Resiliency Act and Secure by Design.

Mr. GARBARINO. Doc.

Mr. MUKKAMALA. I would like to start with an example. Does a radiologist work for a general physician? One is vertical-focused. The other one is horizontal-focused. IT is very horizontal. You've got to maintain your systems.

When it comes to OT, we club it as one thing. It's very vertical-focused and it's a black box. It's very domain-specific. The digital transformation is bringing IT and OT together, and you really see loggerheads. One is: Go patch your system. The other is: With what?

I don't have a firmware patching. I don't have a patching render to patch my firmware. I don't even know what the underlying system is, because I just took a fork from a Linux, stripped it down, and that's my OS drive. I don't know what libraries are in there, because that's not documented.

There's a lot of unknowns when it comes to vertical-focused OT. Again, it comes back to the work force. Are we training cybersecurity folks in water systems?

You're learning on the job. You didn't go through a formal education. Would you ever let a radiology technician come look at a patient without going through a formal certification?

So we have a fundamental gap on how we look at the convergence and what's going on today. Unfortunately, the industry is moving so fast and we will have no choice but IT and OT to work together, and that will also get converged on more generalized. As vendors learn what it is, you'll actually see some vertical training and vertical focus as well.

Mr. GARBARINO. Thank you.

Ms. Adkins, is there anything you wanted to add?

Ms. ADKINS. Yes. I think the one thing we haven't talked about here that really strikes me about OT is we haven't talked about the recoverability story.

The war in Ukraine is an incredible case study for us, as an industry, to see how cyber attacks against their infrastructure are being recovered from and actually how you can negate the effect of a cyber attack if you can recover within minutes or hours.

So while we think about the journey on Secure by Design for OT, we also need to think about the bridge. What are we going to do in the mean time? If that's a 5- to 10-year journey, what's the story for the electric company and the water and whatnot?

I think it has to be some kind of very tough conversation of here's your performance indicator, make sure you can recover the system with the next period of time.

Mr. GARBARINO. Mr. Richberg.

Mr. RICHBERG. Then I think, because I work a lot with these utilities, the challenge is they're regulated utilities, they can identify a need, but they then have to go to a State utilities commission to get the approval to raise the rates in the future to pay for it, so that they're always lagging with resources what they need to fix.

Mr. GARBARINO. I feel like the utility commissions don't always understand what the necessities are.

I am out of my second round of questions. I'll just wait for the Ranking Member, see if he wants to go again.

Yes, yield to Mr. Menendez. We'll go to Laurel first then.

I recognize the gentlewoman from Florida, Ms. Lee, for 5 minutes of questions.

Ms. LEE. Thank you, Mr. Chairman.

Welcome. Thank you all for being here.

Dr. Mukkamala, I'd like to start with a question for you. In your written testimony, you mention the *Forbes* article, "A Trillion-Dollar Global Tech Problem," which talks about the benefits of using automation and streamlining operations, but emphasizes the importance of starting with a thorough audit of existing tools and systems.

Would you tell us a little bit more about why that is the important starting place and how we might use artificial intelligence or other tools to assist us in performing that kind of audit?

Mr. MUKKAMALA. So, Chairwoman Lee, it's a great question.

First, the hypothesis is you need to know what you have, and that's what is missing.

A 2019 audit from the Federal systems clearly identified multiple systems running legacy software with critical vulnerabilities, exposing our country to foreign actors. That is the U.S. Government does routine audits. That's how they identified that.

When you start looking at small businesses, State governments, local governments, higher education, they don't have the resources. They don't even do regular audits unless required by compliance.

If you don't know what you have, you don't know how you can secure that. If I can't secure it, I am running a vulnerable machine.

My simple analogy is: We go do regular checkups at 40. We start when you're born. We stop at 16. We don't go back to a pediatrician. We come back again, start at 40.

Fourteen, 16 years to 40 years, you are a walking time bomb, right? You're hoping you're healthy, you're a superhuman and nothing is going to happen. But 40, suddenly the clock starts, we need to go get our annual done.

For systems, unfortunately, we don't have that. We have to do a continuous thing, not even a periodic. So that's why it's important to go back and take a look at what do I have today and what machine I am on, why am I running on these systems, and then assess how vulnerable you are.

You can't fix everything. Then you have to prioritize what am I going to fix, and then really start building to what we consider resilience.

In an absence of resilience, you have to build mechanisms so you can recover if there is an incident on your organization.

Ms. LEE. Let me interject there, because I think you're touching on something that is very important.

So prior to coming to Congress, I was responsible for running a State agency. One of the greatest challenges that we had was doing exactly what you describe: Identify what are the things that we have, what exists, then how do we deal with all of these legacy systems and their vulnerabilities, and do that in the construct of procurements and the appropriation process?

Government in particular is so poorly suited to be nimble and be efficient and forward-thinking when it comes to integrating new technology and identifying and guarding against those vulnerabilities.

But one of the things that you just mentioned was also recovery. If and when there is an incident, how are we going to get back up to operating?

So I'd love for you to talk about those 2 things in a little more detail.

One is how we should think about navigating away from these legacy systems. Are there good approaches or best practices to trying to identify and then leave them?

Then second, best practices on having that redundancy so that when there's an incident we can continue to operate.

Mr. MUKKAMALA. It's a great question. I am fortunate enough to have a lot of experience working with multiple States and also advising about 6 Governors to that, on the exact topic.

I'll go back to 2008. The State of New Mexico went through a barrage of incidents. Governor Richardson was at the helm of the State. Deloitte was the vendor that was doing annual assessments, charging an arm and a leg, to tell them what they should do and giving PDF reports that nobody would even touch. This is 2008.

Fast forward, 2015. Now we have multiple regulations that States have to comply—actually more regulations than what the Feds think: 1075, CJIS, MRZ, you name it, FERPA, multiple regulations. So they're forced to go do their audits with very limited resources.

The reason they even scan their systems today is because there is an impending Federal audit and I'm going to scan the system. That's not enough.

Today, when you start looking at where the vulnerabilities are, we're still talking vulnerabilities. Unfortunately, vulnerability is too late. We need to be talking about: Do we have coding errors in the software we are developing, co-developing, and using? That's a weakness.

We need to know what weaknesses are that would lead into vulnerabilities. Then we have to look at what are the ones attackers took time to actually develop and exploit. That's weaponization. Then you have to look at it and say: Which are the ones that are already weaponized they're using?

So it's really a life cycle in itself. Most States, I mean, most corporations, are not even equipped.

So that's the space called risk-based vulnerability management, which coined in cyber war in 2008 a project called CACTUS, supported by Congress.

Which vulnerabilities will we use to attack our enemy networks? We turned it around and said: OK, let's go use it for vulnerability prioritization. We created that space in 2011.

Today, that's not enough and we're looking at exposures, weaknesses, because not every vulnerability is patchable; coding errors, somebody has to go modify the code. If I have a vulnerability, if I can patch it, I can patch it.

The stats as of this Monday, there are more than 268,000 known vulnerabilities reported between NVD and other CNAs. There are only 68,000 that are patchable. That is a striking alarm.

So this is becoming a data problem, not a cybersecurity problem. So with States, you're collecting more data than you can consume. That's where AI can really help in being able to consume this data at a faster pace, really prioritize and focus on the critical systems with a functional context. If I'm serving Medicaid, I want to go focus on that system first than trying to focus on a system I'm doing the regular stuff.

To answer your second question, States don't have enough resources for resiliency. They don't operate on N+1 resiliency. I don't have a system-to-system.

That's where recovery becomes a real thing. The basics they focus is back-ups. When in audits, every single time, even the Federal audits, you see systems not being backed up regularly.

So, at the minimum, to really get ahead of ourself from ransomware, we should back any and every critical data, and that should be enforced.

Mr. GARBARINO. The gentlelady's time is expired.

I now recognize the gentlelady from New Jersey, Ms. McIver, for 5 minutes of questions.

Ms. MCIVER. Thank you so much, Chairman. Thank you for allowing me this time.

I want to thank the Ranking Member and our witnesses for joining us today. Of course, today we're here to talk about Secure by Design, an effort aimed to ensuring cybersecurity infrastructure is included in new technologies from the very start.

I represent New Jersey's 10th Congressional District, along with my wonderful colleague here, who represents the Eighth. We have many overlapping cities who experience some cyber attack shutdowns.

Most recently, we had a situation in the city of Hoboken, which I'm sure the Congressman has talked about, and we also experienced something in the city of Newark of different cyber attacks that happened with our Newark Housing Authority as well as our city of Newark City Hall, and we saw some attacks on our health systems as well.

So we continue to see attacks on our State and local governments, small agencies as well. Secure by Design can definitely be able to tackle some of these problems that we see happening with these entities.

So one of my questions to all of the witnesses to answer is: What challenges do you foresee in applying Secure by Design principles to smaller entities such as that I mentioned, whether it's smaller municipalities, smaller health care systems and centers, and underserved and underresourced communities?

Mr. RICHBERG. So Secure by Design is really set up as something the vendors should do, which then the small consumers will be able to benefit from.

I know that the Congresswoman from Florida mentioned procurement. Procurement is the weakness, especially for local government. Those people in the highway department may know if a project is going to be built that's a good bridge. They won't know anything about sensors.

They need those types of things to be built into the product, they need it to be Secure By Design, because those underresourced organizations can't do it.

You mentioned medical. The FDA, under the PATCH Act, is actually a couple of years ahead of CISA in implementing what really looks like Secure by Design with the medical industry, and they're making a lot of strides over the past year.

Ms. MCIVER. Thank you.

Mr. FRY. I think it's a really interesting discussion point, because as we look at Secure by Design affecting vendors, the downstream impact is that these small municipalities won't have to worry as much if their devices are secure.

But it does bring an interesting question of: What are these small municipalities supposed to do today? How can you know, if we assume that suddenly everything is Secure By Design tomorrow, those small municipalities still have to apply updates. They still have to understand what devices and software they even have in their ecosystems.

So they're still going to have to have some focus to understand that I have a secure version of this that I need to update to. That's where advocacy and potentially, you know, funding at the State and Federal level can help those smaller municipalities get to secure systems today.

The faster we can get vendors to do Secure by Design and solve some of these problems today, the faster that funding can be effective or those efforts in those small municipalities can help make their systems more secure.

Ms. MCIVER. Thank you.

Mr. MUKKAMALA. Understanding what they have is the most important thing. The burden needs to be moved from the consumer to the vendor. When we start looking at these 2 fundamental things, we will solve a lot of problems.

The DHS program that's allowing the small municipalities, cities, counties, and public education to look for what vulnerabilities do they have is really helping quite a bit. There's a lot more scanning activity going on on their systems today than ever before.

The recent edition of the E-Rate program, for the first time now public schools can apply for cybersecurity as part of their technology funding. That is a great move by the Congress because that's really going to help those K–12 institutions look for systems that would have impacted kids from learning on-line, because it's very important for rural America.

I mean, New Jersey is blessed because it's urban America. When you look at States like New Mexico, Mississippi, Alabama, these kids can't travel. They have to take on-line classes. If the systems go down, they are out of learning for weeks. We can't afford that. We can't leave children behind because of ransomware.

Ms. MCIVER. Thank you. Thank you so much.

I'm sorry, Ms. Adkins, my time is up.

Thank you so much for that, Chair.

Ms. Adkins, anything to add?

Ms. ADKINS. Yes. Thank you for the question. It's a really good one. I'm sorry to hear what's happening in New Jersey. This is, unfortunately, a plague that we are seeing across many places.

It is possible to build systems that are resistant to ransomware. There are many on the market today, and there will be many more coming as we have this conversation and they come to market.

It's important that through procurement, through consumer choice, that people have access to be able to make those choices, to bring in modern operating systems and modern software. That is ultimately the solution to this problem over the long term.

Ms. MCIVER. Thank you, Ms. Adkins.

I yield the rest—well, no time, but I yield. Thank you.

Mr. GARBARINO. The gentlelady yields back.

I now recognize Mr. Swalwell for his second round of questions.

Mr. SWALWELL. Great. Thank you, Chair.

I just wanted to go back to Dr. Mukkamala.

Your testimony highlighted how GAO has found legacy systems with known vulnerabilities are operating across Federal agencies.

What are the obstacles to upgrading existing legacy technology? How can we address this challenge of insecure legacy systems? How should addressing legacy technology be integrated into Secure by Design?

Mr. MUKKAMALA. So thank you, Ranking Member Swalwell.

The No. 1 fear is breaking the functionality of these legacy systems. I mean, that's where it starts.

The second important thing is the unknown. We don't know what systems we are running. The GAO report talks about it, but we didn't take it further and say: Let's go study the entire Federal complex, civilly and intelligence community, and say, let's catalogue what legacy systems do we have today, what functionality are we serving, and what is the legacy software, who are the vendors they are responsible for?

What's happening that is alarming and interesting is these vendors of legacy software are still charging the Federal Government for support, for maintenance, yet having only 1 or 2 people run a hundred-million-dollar business, and the Federal Government is OK with that.

It's the accountability piece, right? If you're selling me software that's legacy, that's vulnerable, and you have 3 people supporting it, we expect nation-states not to attack us?

So coming back to the question, it's the breaking of it. It's the black box approach and not knowing what's really vulnerable across the Federal ecosystem.

Mr. SWALWELL. Great. Thank you.

Go ahead, Mr. Richberg.

Mr. RICHBERG. I actually would take a different tack on that as a former Federal executive. It's funding. It's resources.

I mean, I remember spending time down in the Chambers explaining the OPM breach, that we had seen something like that coming because we knew we were running a Fortran system that we could not get funded to recapitalize and upgrade.

So, yes, we may have trouble understanding some of the intricacies, but the reality is there are a lot of IT modernization plans that simply don't make the cut to ever be implemented.

Mr. SWALWELL. Great.

Dr. Mukkamala, I get to play like the role of professor here, so go ahead if you want to respond.

Mr. MUKKAMALA. Absolutely, funding is the thing. Then here I'm actually—the Federal Government is already spending money. Yes, we might not get to a modern system because it takes a lot more time, implementation, and it's reworking of the entire process. That's not easy.

That's one of the reasons why people don't get off legacy systems. It's the cost of moving to a newer system. You see that quite a bit not only in the Feds, in the State as well.

The challenge is, if you're paying an IT vendor X dollars, are they really deserving those X dollars? I don't see that being asked.

Mr. SWALWELL. With that, after playing the role of judge or professor, I'm going to yield back to the Chair.

Thank you. Thank you again to all of our witnesses.

Mr. GARBARINO. The gentleman yields back.

I now recognize the gentleman from New Jersey for 5 minutes of questions.

Mr. MENENDEZ. Thank you, Chairman. I yield my 5 minutes to you for additional questions.

Mr. GARBARINO. Oh, thank you, the gentleman. Very kind of you.

Mr. MENENDEZ. I thought you'd appreciate that.

Mr. GARBARINO. Mr. Fry, I wanted to ask you a question.

Your company signed the pledge. What's the benefit of signing the pledge? I mean, it's not like by signing the pledge we'll go along with the pillars, you don't get a stamp of approval saying Secure By Design. So what's the benefit of a company signing the pledge?

Mr. FRY. So I think there's a couple different things that are really important.

For us, as a security company, it's important that we lead by example, just as I've asked the Federal Government to lead by example for acquisitions.

It felt very wrong for us to not be writing our code as much as we could in memory-safe languages, to have the Secure by Design pledge as something that we're doing. It kind-of feels hypocritical to not be doing security as a security company.

So that's really been one of the big driving factors for us, is we've wanted to do this, the pledge. Secure by Design coming out was a good time line to say: Let's do this publicly. So that's been really helpful for us.

The benefit to other companies is that, as all the witnesses today have said, is a more secure ecosystem, and also the ability for security-conscious consumers to decide who they want to buy software and devices from.

They might choose to prioritize security. I hope they would. That's something that we see in the OT space. You're going to be locked in for 20, 30 years with this software, this device. You should buy that more secure version of that. So that's why the pledge is so valuable to us.

Mr. GARBARINO. I have 4 minutes left, and I want you all just to be able to make a closing statement.

So, Mr. Fry, we'll start with you, but if you can just limit it to about a minute, and then we'll go to everybody else, because I know, Mr. Richberg, you wanted to make a comment.

But, Mr. Fry, something you just wanted to make sure is put on the record today, because this is a very important hearing.

Mr. FRY. Yes. I think it's very obvious that Secure by Design is making a lot of waves, but we can't lose sight of the fact that there's software today that is not secure that's deployed in these small governments and utilities and things like that that are going to need security.

We have to do something about the software that's deployed today. We have to make sure that that isn't just the IT systems, that it's got to be the OT systems as well.

So I'd like to call all the OT device manufacturers: Let's do the Secure by Design pledge. Let's work with Congress and find a good way—or CISA—to find a good way to incentivize these companies to actually secure their systems. Because I think limiting it to just IT systems is a little bit shortsighted.

I understand we have to do something that we can do quickly. It's a good first step. But we've got to continue to push further and make that impact across the ecosystem.

Mr. GARBARINO. Thank you.

Ms. Adkins.

Ms. ADKINS. It is technically feasible to solve many of our security problems, but it will require a few things, ingenuity and innovation being almost the easiest of these, the hardest being the work that companies will have to do to rip and replace and what that journey will be like.

We've got trillions of lines of code on the internet. Some portion of that will have to be checked, rewritten, deprecated. Then the systems that actually get deployed are important.

So we need to think not only about the technical components of this, but also the policy components, procurement, the whole ecosystem that plays into how do we make not just digital transformation but the digital retransformation that has to happen.

Mr. GARBARINO. Thank you. Mr. Richberg.

Mr. RICHBERG. To put what Ms. Adkins said slightly another way, the hard stuff is the soft stuff. It's not the technical problem. We have technical fixes for this.

The premise of Secure by Design was that "Field of Dreams" thing, as I said: If you build it, users will flock to it.

Well, my experience from talking to Fortune 500 executives is they don't even know about this. But when you tell them it's here, they say: If I have a choice between product A, B, or C, and one of those is from a company that signed the pledge and is willing to let my people see what they've done to implement it, yes, I'd like to factor that in.

So with a new CISA management, maybe talk about, do we include this in Cybersecurity Awareness Month?

Industry is not going to stop doing this. They weren't mandated to do this. You look at the 251 companies that have signed it. We represent a majority by sales volume, I suspect, of the IT activity in this country. We're doing it because this is good cybersecurity hygiene.

So how do we take advantage of the bully pulpit of letting potential consumers know this is out there, factor this in as you replace your technology.

Mr. GARBARINO. Thank you, Mr. Richberg.

Doctor.

Mr. MUKKAMALA. Secure by Design is a great initiative. We need to continue to do that and to ask for the new Congresses to continue to support it. We have to focus on the fundamentals. What that means is reskilling, upskilling our existing work force.

Secure by Design talks about companies, focusing on the technical aspect. But nowhere in this pledge the people who signed it said: My work force has these gaps today.

We're going to address a fundamental work force problem. I think that absolutely needs to be brought back into first principle thinking on upskilling and reskilling a work force.

Mr. GARBARINO. Thank you very much. Thank you.

Thank you all to the witnesses for coming today and your testimony. I know you've all worked with CISA quite a bit, especially on this. We have as well.

I'm going to miss Director Easterly when she leaves. I know the Ranking Member also worked very well with Director Easterly. I'm looking forward and interested to see who will be taking over CISA next year.

With that, the Members of the subcommittee may have some additional questions for you all, and we would ask that the witnesses respond to those in writing.

Pursuant to committee rule VII(D), the hearing record will be open for 10 days.

Without objection, the subcommittee stands adjourned.

[Whereupon, at 11:29 a.m., the subcommittee was adjourned.]

APPENDIX

Questions From Chairman Andrew R. Garbarino for Heather Adkins

Question 1. Is the Secure by Design initiative effectively driving the cybersecurity ecosystem toward more secure products?

Answer. Response was not received at the time of publication.

Question 2. How would your view of the initiative change if the pledge became mandatory, if at all?

Answer. Response was not received at the time of publication.

Question 3. How do you think Google's decision to pull out of China following Operation Aurora has affected its ability to uphold Secure by Design principles?

Answer. Response was not received at the time of publication.

Question 4a. Which measures from the Secure by Design pledge had your companies already adopted as common practice?

Answer. Response was not received at the time of publication.

Question 4b. What activities or costs did, or will, your companies incur by signing the pledge?

Answer. Response was not received at the time of publication.

Question 5. How does Google apply Secure by Design principles to its AI development and deployment?

Answer. Response was not received at the time of publication.

Question 6. How have you measured your progress when you published reports on implementing Secure by Design?

Answer. Response was not received at the time of publication.

Question 7. Please describe your experience helping CISA draft the pledge. How did you get involved, and what was the drafting process like? Did CISA incorporate your feedback into the pledge's pillars?

Answer. Response was not received at the time of publication.

Question 8. Do you find the guidance documents and advisories CISA has published under the Secure by Design initiative to be valuable? Why or why not?

Answer. Response was not received at the time of publication.

Question 9. As you have implemented Secure by Design principles, have you noticed a significant demand shift from your customers?

Answer. Response was not received at the time of publication.

Question 10. How do you communicate the need for cybersecurity products to your customers?

Answer. Response was not received at the time of publication.

Question 11. How does your company disclose vulnerabilities without increasing risk to your systems?

Answer. Response was not received at the time of publication.

Questions From Chairman Andrew R. Garbarino for Jim Richberg

Question 1. Is the Secure by Design initiative effectively driving the cybersecurity ecosystem toward more secure products?

Answer. Response was not received at the time of publication.

Question 2. How would your view of the initiative change if the pledge became mandatory, if at all?

Answer. Response was not received at the time of publication.

Question 3. Reporting indicates that China-backed actors may have recently exploited vulnerabilities in Fortinet products. As you continue to implement Secure by Design, do you think its pillars will be enough to protect against the China threat?

Answer. Response was not received at the time of publication.

Question 4a. Which measures from the Secure by Design pledge had your companies already adopted as common practice?

Answer. Response was not received at the time of publication.

Question 4b. What new activities or costs did, or will, your companies incur by signing the pledge?

Answer. Response was not received at the time of publication.

Question 5. Recognizing that software and hardware also have unique challenges, do you think CISA made the right choice by leaving out physical products? Why or why not?

Answer. Response was not received at the time of publication.

Question 6. Your company issued progress reports for implementing Secure by Design. How have you measured your progress?

Answer. Response was not received at the time of publication.

Question 7. If you helped CISA draft the pledge, what did was the drafting process like? Did CISA incorporate your feedback into the pledge's pillars?

Answer. Response was not received at the time of publication.

Question 8. Do you find the guidance documents and advisories CISA has published under the Secure by Design initiative to be valuable? Why or why not?

Answer. Response was not received at the time of publication.

Question 9. As you have implemented Secure by Design principles, have you noticed a significant demand shift from your customers?

Answer. Response was not received at the time of publication.

Question 10. How did you communicate the need for cybersecure products to your customers?

Answer. Response was not received at the time of publication.

Question 11. How can the U.S. Government facilitate and incentivize information sharing among vendors in a way that doesn't punish companies for being transparent and optimizes better security for all?

Answer. Response was not received at the time of publication.

Question 12. How does your company disclose vulnerabilities without increasing risk to your systems?

Answer. Response was not received at the time of publication.

Questions From Chairman Andrew R. Garbarino for Shane Paulsen Fry

Question 1. Is Secure by Design initiative effectively driving the cybersecurity ecosystem toward more secure products?

Answer. Response was not received at the time of publication.

Question 2. How would your view of the initiative change if the pledge became mandatory, if at all?

Answer. Response was not received at the time of publication.

Question 3a. Which measures from the Secure by Design pledge had your companies already adopted as common practice?

Answer. Response was not received at the time of publication.

Question 3b. What new activities or costs did, or will, your companies incur by signing the pledge?

Answer. Response was not received at the time of publication.

Question 4. Is every pillar of Secure by Design "specific and measurable"?

Answer. Response was not received at the time of publication.

Question 5. Do you find the guidance documents and advisories CISA has published under the Secure by Design initiative valuable? Why or why not?

Answer. Response was not received at the time of publication.

Question 6. As you have implemented Secure by Design principles, have you noticed a significant demand shift from your customers?

Answer. Response was not received at the time of publication.

Question 7. As a small company, what are the challenges of making cybersecurity a selling point for your products?

Answer. Response was not received at the time of publication.

Question 8. How does your company disclose vulnerabilities without increasing risk to your systems?

Answer. Response was not received at the time of publication.

Questions From Chairman Andrew R. Garbarino for Srinivas Mukkamala

Question 1. Is the Secure by Design initiative effectively driving the cybersecurity ecosystem toward more secure products?

Answer. Response was not received at the time of publication.

Question 2. How would your view of the initiative change if the pledge became mandatory, if at all?

Answer. Response was not received at the time of publication.

Question 3a. Which measures from the Secure by Design pledge had your companies already adopted as common practice?

Answer. Response was not received at the time of publication.

Question 3b. What activities or costs did, or will, your companies incur by signing the pledge?

Answer. Response was not received at the time of publication.

Question 4. Do you find the guidance documents and advisories CISA has published under the Secure by Design initiative to be valuable? Why or why not?

Answer. Response was not received at the time of publication.

Question 5. As you have implemented Secure by Design principles, have you noticed a significant demand shift from your customers or entities you have interacted with?

Answer. Response was not received at the time of publication.

Question 6. How does your company disclose vulnerabilities without increasing risk to your systems?

Answer. Response was not received at the time of publication.

○