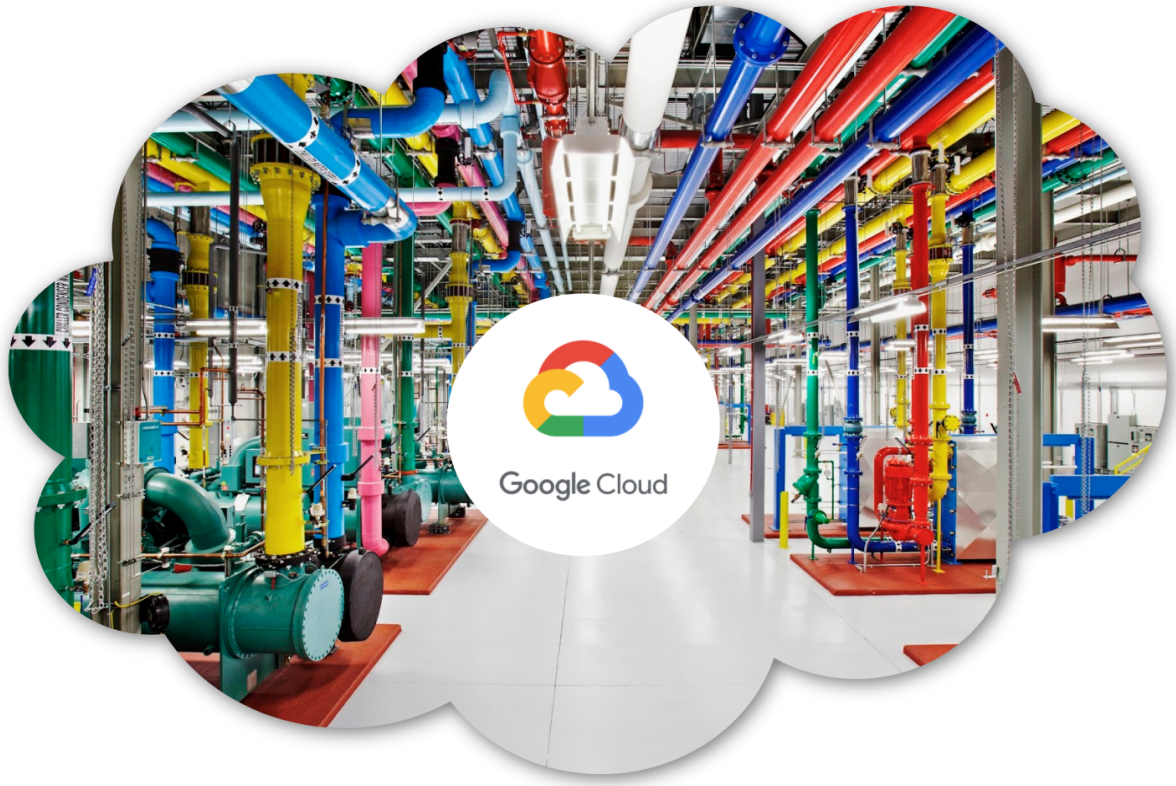
Vendor Contact Details
Company Name: Google LLC
Address: 1600 Amphitheatre Parkway
Mountain View, CA 94043
Website: cloud.google.com

Individual Contact Details
Contact Names: Miles Euell & Kevin Jameson
Title of Contacts: Enterprise Account Executive
Phone: 202-510-3475 & 720-432-2901
Email: mileseu@google.com & kajameson@google.com

Department of Energy
Stewardship of Software for Scientific and
High-Performance Computing
Solicitation #: FR Doc. 2021–23582

December 13, 2021
Submitted to: Hal Finkel
hal.finkel@science.doe.gov



GOOGLE DISCLAIMER: Should you elect to move forward with the purchase of Google products or services, the definitive terms of agreement governing the relevant purchase will be set forth in the applicable Google terms and conditions negotiated and agreed upon by the parties at that time. Please be aware that no terms of any kind, legal or otherwise, contained in your RFI or in Google's response will be binding on either party in any way. Google's responses may be subject to change at any time.

Google Cloud

Table of Contents

1. Request for Information Comments

Google LLC is pleased to respond to the Department of Energy's Request for Information (RFI) - Stewardship of Software for Scientific and High-Performance Computing, dated October 25, 2021, with the following responses to the numbered questions in the RFI.

Google Cloud provides computing resources globally across industries, universities, and public and private sectors. We are engaged with the E4S project to ensure ECP software can build and run on Google Cloud Platform (GCP). At Google Research we design, build and operate warehouse-scale computer systems that are deployed across the globe. We build storage systems that scale to exabytes, approach the performance of RAM, and never lose a byte. We design algorithms that transform our understanding of what is possible.

By providing distributed systems and secured infrastructure, Google can daily benefit the scientific community and participate in making the users of our technologies some of the most productive developers in their fields.

1.1 Software dependencies and requirements for scientific application development and/or research in computer science and applied mathematics relevant to DOE's mission priorities

Current common language and API dependencies of scientific and HPC software include: C, C++, Fortran, Python, MPI, OpenMP, CUDA, and SYCL/DPC++. Common additional software dependencies include Raja, Kokkos, PETSc, Julia, SciPy, and Numpy, among many others.

Researchers are increasingly adopting high-performance data analytics and machine learning software as part of their workflows and even core simulation algorithms. For these, common packages include PyTorch, Tensorflow, R, Apache Spark (and its associated ecosystem). Beyond running these frameworks directly on infrastructure, researchers are increasingly turning to AI, ML, and analytics services. As one example, AutoML services can automatically select and train AI models, reducing the burden on researchers to become AI experts and accelerating their ability to integrate AI capabilities into their research.

Emerging languages, such as JAX, are gaining attention in the scientific and machine learning community as a way to access the power of innovative architectures such as Google's TPU pods.

One emerging trend is that the diversity of frameworks and software packages increases the opportunity for careful matching of infrastructure with workloads within larger workflows. An

associated risk is the inefficiency of future workflows that are constrained to run in a homogeneous hardware environment, both from an application performance perspective and from an infrastructure utilization perspective.

Another key risk stems from the geometrically growing set of combinations of dependent software, such as different compilers, different MPI implementations, CPU-only and CPU+GPU languages, and different math libraries. Building all of the software consistently and correctly is a significant burden for the application developer and a key source of risk. Approaches like Spack repositories that maintain a curated, validated, and signed set of the most common building block combinations, along with automated build systems to generate needed new combinations on demand, can significantly mitigate the risk and improve developer productivity.

Google Cloud provides productive, compatible environments supporting all of these languages, frameworks, and services. It can also mitigate some efficiency risks by providing on-demand access to a variety of workload-optimized environments. This can make it a strong candidate for the underlying infrastructure to host the DOE software stewardship platform.

1.2 Practices related to the security and integrity of software and data

Authors of scientific software must have confidence in how they will protect the security & integrity of their software, the resultant data, and the personal information of their application's users.

The secure software supply chain is critical but the approach to securing software and data is only as strong as the foundation upon which it is built. This is where Google Cloud's world-class infrastructure becomes most relevant. Google runs on privately owned fiber with 140 Points of Presence offering data security by encrypting both in transit and at-rest without traversing public networks. Our Identity and Access Management (IAM) provides fine-grained access at the resource level to enable researchers to secure their software.

We would like to collaborate with DOE to help develop repeatable processes that could be applied across the ECP software ecosystem.

As a cloud pioneer, Google fully understands the security implications of the cloud model. Our cloud services are designed to deliver better security than many traditional on-premises solutions. We make security a priority to protect our own operations, but because Google runs on the same infrastructure that we make available to our customers, their organizations can directly benefit from these protections. That's why we focus on security, and protection of data is among our primary design criteria. Security drives our organizational structure, training priorities and hiring processes. It shapes our data centers and the technology they house. It's

central to our everyday operations and disaster planning, including how we address threats. It's prioritized in the way we handle customer data. And it's the cornerstone of our account controls, our compliance audits and the certifications we offer our customers.

This section outlines Google's approach to security and compliance for Google Cloud, our suite of public cloud products and services, including details on organizational and technical controls regarding how Google protects customer data. Details on compliance and how customers can meet regulatory requirements are covered here.

Google's security culture
Google has created a vibrant and inclusive security culture for all employees. The influence of this culture is apparent during the hiring process, employee onboarding, as part of ongoing training and in company-wide events to raise awareness.

Employee background checks
Before they join our staff, Google will verify an individual's education and previous employment, and perform internal and external reference checks. Where local labor law or statutory regulations permit, Google may also conduct criminal, credit, immigration, and security checks. The extent of these background checks is dependent on the desired position.

Security training for all employees
All Google employees undergo security training as part of the orientation process and receive ongoing security training throughout their Google careers. During orientation, new employees agree to our Code of Conduct, which highlights our commitment to keep customer information safe and secure. Depending on their job role, additional training on specific aspects of security may be required. For instance, the information security team instructs new engineers on topics like secure coding practices, product design and automated vulnerability testing tools. Engineers also attend technical presentations on security-related topics and receive a security newsletter that covers new threats, attack patterns, mitigation techniques and more.

Internal security and privacy events
Google hosts regular internal conferences to raise awareness and drive innovation in security and data privacy, which are open to all employees. Security and privacy is an ever-evolving area, and Google recognizes that dedicated employee engagement is a key means of raising awareness. One example is "Privacy Week," during which Google hosts events across global offices to raise awareness of privacy in all facets, from software development, data handling and policy enforcement to living our privacy principles. Google also hosts regular "Tech Talks" focusing on subjects that often include security and privacy.

Our dedicated security team

Google employs security and privacy professionals, who are part of our software engineering and operations division. Our team includes some of the world's foremost experts in information, application and network security. This team is tasked with maintaining the company's defense systems, developing security review processes, building security infrastructure and implementing Google's security policies. Google's dedicated security team actively scans for security threats using commercial and custom tools, penetration tests, quality assurance (QA) measures and software security reviews.

Within Google, members of the information security team review security plans for all networks, systems and services. They provide project-specific consulting services to Google's product and engineering teams. They monitor for suspicious activity on Google's networks, address information security threats, perform routine security evaluations and audits, and engage outside experts to conduct regular security assessments. We specifically built a full-time team, known as Project Zero, that aims to prevent targeted attacks by reporting bugs to software vendors and filing them in an external database.

The security team also takes part in research and outreach activities to protect the wider community of Internet users, beyond just those who choose Google solutions. Some examples of this research would be the discovery of the POODLE SSL 3.0 exploit and cipher suite weaknesses. The security team also publishes security research papers, available to the public. The security team also organizes and participates in open-source projects and academic conferences.

Our dedicated privacy team

The Google privacy team operates separately from product development and security organizations, but participates in every Google product launch by reviewing design documentation and performing code reviews to ensure that privacy requirements are followed. They help release products that reflect strong privacy standards: transparent collection of user data and providing users and administrators with meaningful privacy configuration options, while continuing to be good stewards of any information stored on our platform. After products launch, the privacy team oversees automated processes that audit data traffic to verify appropriate data usage. In addition, the privacy team conducts research providing thought leadership on privacy best practices for our emerging technologies.

Internal audit and compliance specialists

Google has a dedicated internal audit team that reviews compliance with security laws and regulations around the world. As new auditing standards are created, the internal audit team determines what controls, processes, and systems are needed to meet them. This team facilitates and supports independent audits and assessments by third parties.

Collaboration with the security research community

Google has long enjoyed a close relationship with the security research community, and we greatly value their help identifying vulnerabilities in Google Cloud and other Google products. Our Vulnerability Reward Program encourages researchers to report design and implementation issues that may put customer data at risk, offering rewards in the tens of thousands of dollars. In Chrome, for instance, we warn users against malware and phishing, and offer rewards for finding security bugs. Due to our collaboration with the research community, we've squashed more than 700 Chrome security bugs and have rewarded more than $1.25 million with more than $2 million has been awarded across Google's various vulnerability rewards programs. We publicly thank these individuals and list them as contributors to our products and services.

Operational security

Far from being an afterthought or the focus of occasional initiatives, security is an integral part of our operations.

Vulnerability management

Google administers a vulnerability management process that actively scans for security threats using a combination of commercially available and purpose-built in-house tools, intensive automated and manual penetration efforts, quality assurance processes, software security reviews and external audits. The vulnerability management team is responsible for tracking and following up on vulnerabilities. Once a vulnerability requiring remediation has been identified, it is logged, prioritized according to severity, and assigned an owner. The vulnerability management team tracks such issues and follows up frequently until they can verify that the issues have been remediated. Google also maintains relationships and interfaces with members of the security research community to track reported issues in Google services and open-source tools. More information about reporting security issues can be found at Google Application Security.

Malware prevention

An effective malware attack can lead to account compromise, data theft, and possibly additional access to a network. Google takes these threats to its networks and its customers very seriously and uses a variety of methods to prevent, detect and eradicate malware. Google helps tens of millions of people every day to protect themselves from harm by showing warnings to users of Google Chrome, Mozilla Firefox and Apple Safari when they attempt to navigate to websites that would steal their personal information or install software designed to take over their computers. Malware sites or email attachments install malicious software on users' machines to steal private information, perform identity theft, or attack other computers. When people visit these sites, software that takes over their computer is downloaded without their knowledge. Google's malware strategy begins with infection prevention by using manual

and automated scanners to scour Google's search index for websites that may be vehicles for malware or phishing. Approximately one billion people use Google's Safe Browsing on a regular basis. Google's Safe Browsing technology examines billions of URLs per day looking for unsafe websites. Every day, we discover thousands of new unsafe sites, many of which are legitimate websites that have been compromised. When we detect unsafe sites, we show warnings on Google Search and in web browsers. In addition to our Safe Browsing solution, Google operates VirusTotal, a free online service that analyzes files and URLs enabling the identification of viruses, worms, trojans and other kinds of malicious content detected by antivirus engines and website scanners. VirusTotal's mission is to help in improving the antivirus and security industry and make the Internet a safer place through the development of free tools and services.

Google makes use of multiple antivirus engines in Gmail, Drive, servers and workstations to help identify malware that may be missed by antivirus signatures.

Monitoring

Google's security monitoring program is focused on information gathered from internal network traffic, employee actions on systems and outside knowledge of vulnerabilities. At many points across our global network, internal traffic is inspected for suspicious behavior, such as the presence of traffic that might indicate botnet connections. This analysis is performed using a combination of open-source and commercial tools for traffic capture and parsing. A proprietary correlation system built on top of Google technology also supports this analysis. Network analysis is supplemented by examining system logs to identify unusual behavior, such as attempted access of customer data. Google security engineers place standing search alerts on public data repositories to look for security incidents that might affect the company's infrastructure. They actively review inbound security reports and monitor public mailing lists, blog posts, and wikis. Automated network analysis helps determine when an unknown threat may exist and escalates to Google security staff, and network analysis is supplemented by automated analysis of system logs.

Incident management

We have a rigorous incident management process for security events that may affect the confidentiality, integrity, or availability of systems or data. If an incident occurs, the security team logs and prioritizes it according to its severity. Events that directly impact customers are assigned the highest priority. This process specifies courses of action, procedures for notification, escalation, mitigation, and documentation. Google's security incident management program is structured around the NIST guidance on handling incidents (NIST SP 800–61). Key staff are trained in forensics and handling evidence in preparation for an event, including the use of third-party and proprietary tools. Testing of incident response plans is performed for key areas, such as systems that store sensitive customer information. These tests take into consideration a variety of scenarios, including insider threats and software

vulnerabilities. To help ensure the swift resolution of security incidents, the Google security team is available 24/7 to all employees. If an incident involves customer data, Google or its partners will inform the customer and support investigative efforts via our support team. We outline Google's end-to-end data incident response process in our whitepaper.

Technology with security at its core

Google Cloud runs on a technology platform that is conceived, designed and built to operate securely. Google is an innovator in hardware, software, network and system management technologies. We custom-designed our servers, proprietary operating system, and geographically distributed data centers. Using the principles of "defense in depth," we've created an IT infrastructure that is more secure and easier to manage than more traditional technologies.

State-of-the-art data centers

Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, and biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. As you get closer to the data center floor, security measures also increase. Access to the data center floor is only possible via a security corridor which implements multi-factor access control using security badges and biometrics. Only approved employees with specific roles may enter. Less than one percent of Googlers will ever set foot in one of our data centers.

Powering our data centers

To keep things running 24/7 and ensure uninterrupted services, Google's data centers feature redundant power systems and environmental controls. Every critical component has a primary and alternate power source, each with equal power. Diesel engine backup generators can provide enough emergency electrical power to run each data center at full capacity. Cooling systems maintain a constant operating temperature for servers and other hardware, reducing the risk of service outages. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, and smoke detectors trigger audible and visible alarms in the affected zone, at security operations consoles, and at remote monitoring desks.

Environmental impact

Google reduces the environmental impact of running our data centers by designing and building our own facilities. We install smart temperature controls, use "free-cooling" techniques like using outside air or reused water for cooling, and redesign how power is distributed to

reduce unnecessary energy loss. To gauge improvements, we calculate the performance of each facility using comprehensive efficiency measurements. We're the first major Internet services company to gain external certification of our high environmental, workplace safety and energy management standards throughout our data centers. Specifically, we received voluntary ISO 50001 certification and incorporated our own protocols to go beyond standards.

Custom server hardware and software

Google's data centers house energy-efficient, custom, purpose-built servers and network equipment that we design and manufacture ourselves. Unlike much commercially available hardware, Google servers don't include unnecessary components such as video cards, chipsets, or peripheral connectors, which can introduce vulnerabilities. Our production servers run a custom-designed operating system (OS) based on a stripped-down and hardened version of Linux. Google's servers and their OS are designed for the sole purpose of providing Google services. Server resources are dynamically allocated, allowing for flexibility in growth and the ability to adapt quickly and efficiently, adding or reallocating resources based on customer demand. This homogeneous environment is maintained by proprietary software that continually monitors systems for binary modifications. If a modification is found that differs from the standard Google image, the system is automatically returned to its official state. These automated, self-healing mechanisms are designed to enable Google to monitor and remediate destabilizing events, receive notifications about incidents, and slow down potential compromise on the network.

Hardware tracking and disposal

Google meticulously tracks the location and status of all equipment within our data centers from acquisition to installation to retirement to destruction, via barcodes and asset tags. Metal detectors and video surveillance are implemented to help make sure no equipment leaves the data center floor without authorization. If a component fails to pass a performance test at any point during its lifecycle, it is removed from inventory and retired. Google hard drives leverage technologies like FDE (full disk encryption) and drive locking, to protect data at rest. When a hard drive is retired, authorized individuals verify that the disk is erased by writing zeros to the drive and performing a multiple-step verification process to ensure the drive contains no data. If the drive cannot be erased for any reason, it is stored securely until it can be physically destroyed. Physical destruction of disks is a multistage process beginning with a crusher that deforms the drive, followed by a shredder that breaks the drive into small pieces, which are then recycled at a secure facility. Each data center adheres to a strict disposal policy and any variances are immediately addressed. We outline Google's end-to-end data deletion process in our whitepaper.

A global network with unique security benefits

Google's IP data network consists of our own fiber, public fiber, and undersea cables. This allows us to deliver highly available and low latency services across the globe.

In other cloud services and on-premises solutions, customer data must make several journeys between devices, known as "hops," across the public Internet. The number of hops depends on the distance between the customer's ISP and the solution's data center. Each additional hop introduces a new opportunity for data to be attacked or intercepted. Because it's linked to most ISPs in the world, Google's global network improves the security of data in transit by limiting hops across the public Internet.

Defense in depth describes the multiple layers of defense that protect Google's network from external attacks. Only authorized services and protocols that meet our security requirements are allowed to traverse it; anything else is automatically dropped. Industry-standard firewalls and access control lists (ACLs) are used to enforce network segregation. All traffic is routed through custom GFE (Google Front End) servers to detect and stop malicious requests and Distributed Denial-of-service (DDoS) attacks. Additionally, GFE servers are only allowed to communicate with a controlled list of servers internally; this "default deny" configuration prevents GFE servers from accessing unintended resources. Logs are routinely examined to reveal any exploitation of programming errors. Access to networked devices is restricted to authorized personnel.

Securing data in transit

Data is vulnerable to unauthorized access as it travels across the Internet or within networks. For this reason, securing data in transit is a high priority for Google. The Google Front End (GFE) servers mentioned previously support strong encryption protocols such as TLS to secure the connections between customer devices and Google's web services and APIs. Cloud customers can take advantage of this encryption for their services running on Google Cloud Platform by using the Cloud Load Balancer. Google Cloud Platform also offers customers additional transport encryption options, including Cloud VPN for establishing IPSec virtual private networks. Our encryption in transit whitepaper and application layer transport security whitepaper provide more in-depth information on this topic.

Low latency and highly available solution

Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and Internet connectivity, and the software services themselves. This "redundancy of everything" includes the handling of errors by design and creates a solution that is not dependent on a single server, data center, or network connection. Google's data centers are geographically distributed to minimize the effects of regional disruptions on global products such as natural disasters and local outages. In the event of hardware, software, or network failure, platform services and control planes are automatically and instantly shifted from one facility to another so that platform services can continue without interruption. Google's highly redundant infrastructure also helps customers protect themselves from data loss. Google Cloud Platform resources can be created and

deployed across multiple regions and zones. Allowing customers to build resilient and highly available systems.

Our highly redundant design has allowed Google to achieve an uptime of 99.984% for Gmail for the last years with no scheduled downtime. Simply put, when Google needs to service or upgrade our platform, users do not experience downtime or maintenance windows.

Service availability

Some of Google's services may not be available in some jurisdictions. Often these interruptions are temporary due to network outages, but others are permanent due to government-mandated blocks. Google's Transparency Report also shows recent and ongoing disruptions of traffic to Google products. We provide this data to help the public analyze and understand the availability of online information.

Independent third-party certifications

Google Cloud provides a number of third-party certifications, detailed here.

Data usage

Our philosophy

Google Cloud customers own their data, not Google. The data that customers put into our systems is theirs, and we do not scan it for advertisements nor sell it to third parties. We offer our customers a detailed data processing amendment for GCP and G Suite, both of which describe our commitment to protecting customer data. It states that Google will not process data for any purpose other than to fulfill our contractual obligations. Furthermore, if customers delete their data, we commit to deleting it from our systems within 180 days. Finally, we provide tools that make it easy for customers to take their data with them if they choose to stop using our services, without penalty or additional cost imposed by Google. Read our Trust Principles to learn more about Google Cloud's philosophy and commitments to customers.

Data access and restrictions

Administrative access

To keep data private and secure, Google logically isolates each customer's data from that of other customers and users, even when it's stored on the same physical server. Only a small group of Google employees have access to customer data. For Google employees, access rights and levels are based on their job function and role, using the concepts of least-privilege and need-to-know to match access privileges to defined responsibilities. Google employees are only granted a limited set of default permissions to access company resources, such as employee email and Google's internal employee portal. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as dictated by Google's security policies. Approvals are managed by workflow tools that maintain audit records of all changes. These tools control both the

modification of authorization settings and the approval process to ensure consistent application of the approval policies. An employee's authorization settings are used to control access to all resources, including data and systems for Google Cloud products. Support services are only provided to authorized customer administrators whose identities have been verified in several ways. Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams, and we provide audit logs to customers through Access Transparency for GCP.

For customer administrators

Within customer organizations, administrative roles and privileges for Google Cloud are configured and controlled by the project owner. This means that individual team members can manage certain services or perform specific administrative functions without gaining access to all settings and data.

Law enforcement data requests

The customer, as the data owner, is primarily responsible for responding to law enforcement data requests; however, like other technology and communications companies, Google may receive direct requests from governments and courts around the world about how a person has used the company's services. We take measures to protect customers' privacy and limit excessive requests while also meeting our legal obligations. Respect for the privacy and security of data you store with Google remains our priority as we comply with these legal requests. When we receive such a request, our team reviews the request to make sure it satisfies legal requirements and Google's policies. Generally speaking, for us to comply, the request must be made in writing, signed by an authorized official of the requesting agency and issued under an appropriate law. If we believe a request is overly broad, we'll seek to narrow it, and we push back often and when necessary. For example, in 2006 Google was the only major search company that refused a U.S. government request to hand over two months of user search queries. We objected to the subpoena, and eventually a court denied the government's request. In some cases we receive a request for all information associated with a Google account, and we may ask the requesting agency to limit it to a specific product or service. We believe the public deserves to know the full extent to which governments request user information from Google. That's why we became the first company to start regularly publishing reports about government data requests. Detailed information about data requests and Google's response to them is available in our Transparency Report and government requests whitepaper. It is Google's policy to notify customers about requests for their data unless specifically prohibited by law or court order.

Third-party suppliers

Google directly conducts virtually all data processing activities to provide our services. However, Google may engage some third-party suppliers to provide services related to Google Cloud, including customer and technical support. Prior to onboarding third-party

suppliers, Google conducts an assessment of the security and privacy practices of third-party suppliers to ensure they provide a level of security and privacy appropriate to their access to data and the scope of the services they are engaged to provide. Once Google has assessed the risks presented by the third-party supplier, the supplier is required to enter into appropriate security, confidentiality, and privacy contract terms.

Regulatory compliance

Our customers have varying regulatory compliance needs. Our clients operate across regulated industries, including finance, pharmaceutical and manufacturing.

Our most up-to-date compliance information is available here.

Sharing supply chain security solutions industry-wide

The Executive Order on Improving the Nation's Cybersecurity highlighted the criticality of the software supply chain. As part of this process, Google has submitted papers on artifact integrity and the importance of verifiable metadata to address supply chain security. A summary of these papers and links to the full statements can be found here, with particularly relevant excerpts below:

> **Software Supply Chain Integrity**
>
> Google strongly encourages adoption of SLSA, an end-to-end framework for ensuring the integrity of software artifacts throughout the software supply chain. Four "SLSA Levels" provide incrementally adoptable guidelines that each raise the bar on security standards for open-source software.
>
> SLSA is based on Google's internal framework Binary Authorization for Borg (BAB) that ensures that all software packages used by the company meet high integrity standards. Given BAB's success, we have adapted the framework to work for systems beyond Google and released it as SLSA to help protect other organizations and platforms.
>
> We have shared many of Google's practices for security and reliability in our Site Reliability Engineering book. Following our recent introduction of SLSA to the wider public, we are looking forward to making improvements in response to community feedback.
>
> **Minimum Requirements for Software Bills of Materials (SBOM)**
>
> Google submitted an additional paper in response to the NTIA's request for comments on creating SBOMs, which will give users information about a software package's contents. Modern development requires different approaches than classic packaged software, which means SBOMs must also deal with intermediate artifacts like containers and library dependencies.

SBOMs need a reasonable signal-to-noise ratio: if they contain too much information, they won't be useful, so we urge the NTIA to establish both minimum and maximum requirements on granularity and depth for specific use-cases. We also recommend considerations for the creation of trustworthy SBOMs, such as using verifiable data generation methods to capture metadata, and preparing for the automation and tooling technologies that will be key for widespread SBOM adoption.

In conclusion, the protection of customer data is a primary design consideration for all of Google's infrastructure, products and personnel operations. Our scale of operations and collaboration with the security research community enable Google to address vulnerabilities quickly or prevent them entirely.

We believe that Google can offer a level of protection that very few public cloud providers or private enterprise IT teams can match. Because protecting data is core to Google's business, we can make extensive investments in security, resources and expertise at a scale that others cannot. Our investment frees customers to focus on their business and innovation. Data protection is more than just security. Google's strong contractual commitments make sure customers maintain control over their data and how it is processed, including the assurance that their data is not used for advertising or any purpose other than to deliver Google Cloud services.

For these reasons and more, over five million organizations across the globe, including 64 percent of the Fortune 500, trust Google with their most valuable asset: their information. Google will continue to invest in our platform to allow customers to benefit from our services in a secure and transparent manner.

1.3 Infrastructure requirements for software development for scientific and high-performance computing

We acknowledge that HPC and scientific software is built against a variety of libraries and tools with common functionality, and that the community currently utilizes build systems such as OpenHPC for needed combinations & binaries and Spack for intelligent graph dependency algorithms in shared repos. We believe it will be important to study Spack and collaboratively explore with the DOE how Google's single source tree approach may also be leveraged to solve similar problems.

Google Software Development Infrastructure

Google's approach utilizes an extensively built infrastructure in order to support our software systems that enable software development at an unprecedented scale. Many of these innovations are detailed in the "Software Engineering at Google" book. These systems have been optimized to use commodity hardware and built-in fault tolerance. We have a long history of releasing our software as open source to advance the state of cluster management, distributed file systems, and machine learning. Google uses a single build system for the entire company called Bazel, and allows Google to build fully hermetic binaries at any time. Bazel is also connected to a remote distributed compiler infrastructure that allows engineers to build software that can compile in minutes what would normally take hours to compile on a single machine. This allows us to move quickly, and make sure that the binaries we build matches the code in the code repository. The entire code base also uses the build system to run tests; which means that any change in the code repository including third party code can be used to test changes across the entire code base. This has allowed us to catch issues in third party software that were caught by internal Google test cases for binaries that use those dependencies.

Our source code is indexed by our internal code search tool to allow faster searches about and between source code. Our search tools utilize the build system to index cross references by using the ASTs generated during compilation. We open sourced this system as Kythe, which relies on having modifiable parsers for the languages we support in our code base.

Google relies on distribution with commodity hardware rather than specialized hardware to provide fast experiences for our users and our developers. That is true for everything from Google Search, Google Cloud and scientific computing.

Open Source Software – Google Infrastructure

Google is heavily involved in the open source community, and because of this, we have built additional infrastructure around managing contributors and effectively building, releasing, and testing open source software without relying on Google infrastructure.

We frequently utilize GitHub as a publicly-available venue to share artifacts, track issues, and collaborate with the community of contributors. For larger projects like Android and Chromium, we utilize Gerrit, an open source collaboration tool that integrates the Git distributed version control system.

Required Key Capabilities Not Already Present: Hardware Development

More open source Process Design Kits (PDKs)

We believe that by making foundry PDKs (the sets of basic requirements and building blocks for designing chips that can be manufactured at a specific foundry) more accessible via open

source licenses, commercial demand for these foundries is significantly increased. When applied to domestic US foundries, this increased demand allows the foundry to benefit from economies of scale, lower costs for their customers, and encourages robust user communities to form around them. Google has demonstrated this hypothesis with SkyWater Technology: by making the SkyWater 130nm PDK available under an open source license, demand has skyrocketed. By extending this approach to support multiple processes and pairing them with expanded tooling and "building block" primitives, designers gain the ability to more easily convert chip designs between different manufacturing processes, whether to take advantage of better power efficiencies at smaller nodes, lower manufacturing costs at larger nodes, or even to shift production based on foundry availability without needing to redesign from scratch.

Opening up technology access to more advanced manufacturing nodes like 90nm, 65nm 45nm, 22nm, 12nm, and 7nm will help advance the state of open source hardware IP, and assist basic research by allowing more IP sharing between research groups that require advanced sensors or electronics. These steps are needed in order to continue advancing the capabilities of technology in the United States. We believe doing so will pay hefty dividends to the country, and our company which is why we've already invested in this approach.

Open source implementations and or generators of chiplet standards

The market currently lacks voluntary technical standards for chiplets that could further increase flexibility, competition, and give designers more options in their choice of suppliers. Unfortunately, this is a "chicken and egg" problem: chiplet suppliers won't manufacture chiplets if there is no demand, customers won't design using chiplets until they are available for purchase, and even if one company offered a chiplet solution, customers don't want to be locked into a single source for chiplets and their packaging.

Although numerous efforts exist in this area (AXI, CXL, AIB, etc.), the licensing restrictions applied to either the standards themselves or their resulting implementations present a barrier to any one standard gaining traction in the industry. Further, their proprietary nature means that any research conducted in this area cannot be openly distributed to the broader HPC community. The creation and subsequent availability of an open source implementation of a chiplet standard would enable researchers to publish results that are more easily verifiable, reproducible, and would kickstart an ecosystem around said chiplet standard.

Open source place and route tools

Open source compilers for C and C++ were major contributors to the software revolution of the early 2000s. Without these tools, it's likely that many of the most impactful open source projects like Linux, Python, Ruby, OpenSSL and Blender would never have come to fruition. These open source tools eventually surpassed their proprietary counterparts with far less resources and no single point of coordination.

Today, projects like OpenROAD are providing the same opportunity but in the hardware space instead of software. Projects like these need contributions and support to get off the ground and to usher in the next great hardware revolution. Small amounts of funding here could have dramatic impacts on the state of hardware, software and the country.

HPC EDA (Electronic Design Automation) software

EDA software is often known for its long turnaround times that can often be measured in days. This actively reduces the rate of innovation to a near standstill. Hardware projects often have a 1 to 2 year life cycle, which means that engineers might only get fifty or a hundred total attempts at producing a piece of hardware. This low speed feedback loop directly impacts the rising cost of producing advanced silicon and its perceived risks.

Much of this slowness is due to the underlying software being optimized for single machine or even single CPU runtime environments. To create the next generation of hardware, we believe that it's key to fund projects to enable the use of HPC capabilities to solve EDA problems in minutes instead of weeks. Google is certain that in the next 1-2 years, these innovations will be required to keep pace.

Autotuning for complex parameter spaces

EDA software is often so complex that it can require hundreds of flags with esoteric values to produce working silicon. This can often be a major obstacle to working silicon, and can only be mitigated with experimentation and as mentioned earlier, attempting experiments with EDA tools can often involve incredibly long cycle times.

To mitigate these complex parameter spaces, it will be important to take advantage of black box optimizers that can find good sets of parameters using user-defined metrics. This will become important within the next year as non-traditional hardware designers adopt open source EDA tools like OpenROAD. Investing in this technology can drastically reduce the time required to build working hardware.

More advanced open source hardware synthesis tools

While still unconfirmed, we know that the open source synthesis tools like Yosys struggle with mapping Verilog and other HDL languages to ASIC standard cell libraries at the same quality as commercial tools.

Open source users have reported that they aren't satisfied with the performance of synthesis tools, and would like to see more advanced methods used to better take advantage of the silicon. Synthesis has a tremendous impact on the total performance of the hardware because it is the first stage in the hardware flow; a poor synthesis result can reduce the performance of your silicon by half or more. Investing more resources into hardware synthesis will immediately help open source EDA tools better address the hardware market.

Hardware Package Managers

Early research should be invested into hardware package managers. These package managers should mirror the functionality offered by software package managers like npm, maven, and apt. Ideally, they should offer versioning, easy importing, and publishing. With the expanding ecosystem of fully open source silicon, it will become more important to index these designs and to make sure that they are easy to integrate quickly. This will become more important in the next 2-3 years as the open source IP market grows.

IP Generators

We need more robust IP generators for complex IO components like:

- SerDes,
- Phase locked loops (PLLs),
- Analog to digital converters (ADC),
- Digital to analog converters (DAC),
- DDR[1-5] memory controllers,
- SRAM generators,
- Radio applications, and
- Temperature sensors and power meters.
- Power controllers
- Network on a chip
- Digital signal processors
- eFPGAs
- USB interfaces
- PHYs

The above IP components are difficult to build, and would greatly benefit from additional use case specific customization. Allowing these components to be generated on the fly would allow faster development times as compared to the commercial IP available. The IP generators listed above are needed to build SoCs that address the needs of the market in the next 1-3 years with high confidence. In particular SerDes, PLLs, ADCs, DACs, DDR[3-5] memory controllers, SRAM generators are needed immediately to address the current market's needs.

Faster and more robust verification tools

A key part of hardware development is the verification tools, which is currently the weakest part of the open source hardware tool story. We need massive investments into:

- Layout vs. synthesis tooling,
- Parasitic extraction tooling,
- Open source static timing engines that support CCS models,
- TSMC open model interface support in Xyce,
- sSan chain support in EDA tools,

- Fast HPC based logic simulators, and
- Formal verification tooling.

These tools directly impact working silicon, and everyday we go without them is actively hampering the capabilities of the open source ecosystem.

1.4 Developing and maintaining community software

Google has a long history of developing, releasing, and using open source software. That history is rooted in Google's technology and economic perspective; using and releasing open source software brings benefits in internal developer productivity, customer requirements, and industry-wide computing advancement. Google's Chief Economist Hal Varian said, "Open data and open source are good not only for us and our industry, but also benefit the world at large."[1].

Google's Open Source Programs Office consults Alphabet and Cloud Customers on open source best practices. We offer several resources listed below to help project owners determine their project's business goal, open source strategy, and plan for sustainably developing and maintaining community software. In addition to the resources below, the Open Source Programs Office supports our trusted partnerships with Cloud customers by hosting briefings and workshops with our open source experts.

Open Source Stewardship Guide

There is a lifecycle for developing and maintaining community software that Google likens to a tree's growth lifecycle. The phases are Seed, Sprout, Sapling, Mature. At each phase, the project owner needs to ask key questions and take certain actions to help the project mature.

Appendix A is Google's Open Source Project Stewardship Guide, which details the key questions to ask and actions to take at each stage in order to help the project mature.

Google Open Source Practices

As a thought leader in the open source industry and deeply committed open source citizen, Google publishes how it releases open source software and manages community contributions on opensource.google/docs. We provide this transparency to share our 20+ years of hard earned expertise so others can accelerate their own learning and be able focus more of their energy on creating their own successful open source projects. Today, other companies managing their teams' open source efforts broadly reference this resource.

1.5 Challenges in building a diverse workforce and maintaining an inclusive professional environment

Google is committed to continuing to make diversity, equity, and inclusion part of everything we do—from how we build our products to how we build our workforce.

Google is growing to satisfy that vision. In the past few years, we've doubled in size—today, we have more than 100,000 employees in 170 cities spanning nearly 60 countries. Operating at this scale brings an elevated level of responsibility to everything we do—including a workforce that's more representative of our users, and a workplace that creates a sense of belonging for everyone.

As Google continues to grow, we have a responsibility to scale our diversity, equity, and inclusion initiatives to increase pathways to tech in the communities we call home. Here's how we're approaching that work.

We are building a robust, diverse talent pool to support our industry's growth. By providing computer science education from primary school through university we are growing the next generation of Black and Latinx tech leaders through programs like CS First, Code Next, and Tech Exchange.
Google works hard to attract the best talent and once they are here, we want them to stay. To support this, we build diversity, equity, and inclusion capabilities among all Googlers from managers and leaders, to front line human resources. The Equity Programs Team focuses on ensuring parity in how we source and hire Nooglers and in performance reviews, promotions, and retention. Through our Employee Resource Groups, Leadership Councils, and Diversity councils, we foster a sense of belonging throughout the company, even while many of us are working from home.

Responsible growth means looking beyond the demands of our industry, to consider how our work impacts the cities, sites, and countries where we operate. We approach this work by building long-term partnerships with educational institutions, policymakers, and community organizations. Google.org is committed to philanthropy in support of STEM access for underserved communities. Grow With Google's Digital Coaches provide digital skills training and coaching to help Black and Latinx small businesses grow.

See: Google 2021 Diversity Annual Report

1.6 Requirements, barriers, and challenges to technology transfer, and building communities around software projects, including forming consortia and other non-profit organizations

In areas where Google seeks to support existing or developing standards or technologies, or to develop a healthy community of contributors and increase adoption, we frequently create or join open source foundations. These are non-profit organizations created to provide governance and stewardship of an open source project or technology standard. Benefits vary by foundation, but many provide a vendor-neutral location for relevant copyright, trademarks, and other IP. Some foundations provide further benefits such as technical mentorship for projects, community development, and project marketing.

In nearly all cases, active participation is necessary to benefit from creating or joining a foundation. This can include something as simple as being an active developer on a given project, serving on governing, technical or other committees, or participating in events, community management, and marketing activities.

When Google transfers an open source project to a foundation, typically the software source code is only licensed to the foundation, which is not a transfer of ownership. Foundation participants often continue to own copyright and patents in their contributions, even under different licenses. There is generally no net legal effect to transferring management of a project, because the project's copyrights and patents were already licensed under the terms of the project's open source license. Where applicable, trademarks may be the only thing that changes ownership to the open source foundation, but other changes could include the hosting of repositories, internet domains, or community engagement tools such as Slack, Google Groups, Discord servers, etc.

When forming open source foundations, many elements must be considered to provide sustainable stewardship of the project. One key ingredient is governance of the foundation, to ensure that both strategic project and participant goals are met. For participants in open source foundations, developing healthy communities requires yielding control over time as the culture of the project gels around strong leadership, finding a balance between individual participant control and community growth.

Other ingredients that are required to set up and sustain a foundation include:

- Legal services to establish the nonprofit and manage the project trademarks;
- Funding to seed and sustain the foundation staffing, operations, and programs;
- Financial services to prepare the annual nonprofit 990 tax form or manage other tax filings or payrolls for any paid members;
- Clarity on who executes the foundation's operation and programs (e.g. Executive Director and other staff);

- Clarity on the boards' roles vs. the staff's roles;
- Clarity on how decisions are made and the role that the board, staff, and community have with decisions.

1.7 Overall scope of the stewardship effort

We believe the potential scope described in the RFI to be sufficient and robust for serving ASCR's stewardship efforts. Additional feedback in the form of key questions to consider is provided in our Open Source Project Stewardship Guide, referenced in Section 4 of this response and included as an appendix.

1.8 Management and oversight structure of the stewardship effort

Similar to other efforts to develop standards or technologies in which we participate, we anticipate the most effective model for management and oversight to be in the form of an existing or newly-created open source foundation, with a governance body that consists of DOE stakeholders, federally-funded research and development centers, academic researchers, and interested commercial industry partners.

We do not have any specific recommendations around the management of DOE facilities and their relevant testbed systems. However, we suggest that alternative access models should also be considered, including the funding of resources or time on equivalent HPC infrastructure that can be hosted on commercially-available cloud providers, or the funding of shared resources to increase accessibility to community members who would otherwise be unable to participate in research. Google has demonstrated a similar approach through the funding of multi-project wafer shuttles for semiconductor manufacturing. Under this model, a single manufacturing run at a foundry is purchased, but instead of replicating a single design across a silicon wafer in large quantities, multiple projects are combined together and manufactured in smaller sample quantities. By allocating design "slots" to members of the open source community, participants who would be otherwise unable to afford their own dedicated manufacturing run to validate their designs are able to further their research. Google utilized this approach to drive community adoption of the open source SkyWater 130nm process design kit (PDK) and as a means to test open source chip design workflows in a fully end-to-end manner. When SkyWater and Google ran the first multi-project wafer (MPW) shuttle run after release of the open source PDK, we received 45 design submissions in only 30 days, indicating significant interest from both commercial industry (including Western Digital and IBM) and academia. 60% were from first-time designers.

1.9 Assessment and criteria for success for the stewardship effort

Measuring the success of a software stewardship effort is complex and filled with nuance. The metrics and criteria used will differ depending on who is performing the stewardship and contributing, because the economic incentives and contribution models are unique between Government agencies, FFRDCs, academia, and collaborations with commercial industry.

Although sweeping generalizations and estimates can be made about first-order costs on work like code reviews, such as the equivalent hourly pay or time invested in a given review, this fails to account for the social and community investment made by the same code reviewer to work with a new committer to onboard them to a project, help them track down bugs, and other sponsorship work which cannot be captured by this metric. We have instead shifted to an input-output model which examines investments into a larger system and the impacts we can show from these investments. We utilize KPIs, a specific kind of metric to measure pulse points that correlate to a process, program, or product being considered to be successful.

As "success" itself is a subjective measure, we first work to define what success looks like for the program's stakeholders, which could come from their organizational mission or vision, their business goals, shared roadmaps, or shared dashboards to understand what they track and why. From these, we work to identify objectives, define observable aspects, establish a baseline, define our desired trend, and then determine signal phenomena. An example of this approach is shown in our annual analysis of Google's contributions to open source. This is centered on Google Open Source's mission to "bring the value of open source to Google and the resources of Google to open source," explicitly outlines data samples and evolving methodology, and applies quantitative and qualitative methods.

Further, we would also like to recommend and highlight the work of Community Health Analytics Open Source Software (CHAOSS), a Linux Foundation project focused on creating analytics and metrics to help define community health. Their metrics definitions are available at https://chaoss.community/metrics/.

1.10 Other - What are key obstacles, impediments, or bottlenecks to progress by, and success of, future development of software for scientific and high performance computing?

The Challenges associated with building large-scale, resilient software to solve real problems in scientific computing is a significant one. That said, workflows and scientific campaigns can be made resilient, where thousands of smaller calculations can be run as a herd, with failing elements restarted.

While this isn't a truly difficult problem, it will be a hurdle for the scientific community as most researchers largely are not expert software engineers.

One final impediment we could consider is the growing integration of scientific applications with scientific instruments and the need for heterogeneous environments and high-speed data access. This is another area where cloud's network and resource heterogeneity and agility can be helpful.