ANNUAL REPORT
2021 - 2022

Board Members

Alexander Jäger
Javier Berciano
Tracy Bills
Serge Droz
Sherif Hashem
Michael Hausding (CFO)
Mona Elisabeth Østvang
Shawn Richardson
Dave Schwartzburg
Yukako Uchida

FIRST™
Improving Security Together

Introductory Letter

Dear Reader,

The world was still amid a pandemic in early 2022, but there was a sentiment of hope that things would get better. Then the Ukraine conflict happened. This invasion is a deeply sad moment for our members and me. Some of us may have colleagues who are directly affected, friends or family in eastern Europe, and feel deep empathy for those affected.

FIRST is a global community tied together by a shared mission and motivation to bring together incident response teams and security teams from every country across the world to ensure a safe internet for all. We are also tied together as citizens of the world. Our role is to provide incident responders with the means to find the right teams and information, achieve a common understanding, and help technical and non-technical communities understand what we all do. All of this becomes even more important in crises. While we had to act upon sanctions issued by the US Government to temporarily suspend all member organizations originating in Russia and Belarus, we firmly believe that incident responders should be kept out of conflict.

Even amid difficulties, we continued to hold multiple virtual events, which enabled us to connect with harder-to-reach regions and teams than before. I look forward to seeing how we can continue in this vein and return to in-person events. I am incredibly grateful for all the efforts to elevate FIRST as an organization. The recent addition of two new permanent professional staff will help us continue to play an essential role in the international community to "make sure others understand what we do, and enable us rather than limit us."

Let me end by thanking all of FIRST's staff and volunteers who helped us and dedicated their energy. I am thankful to be part of our community.

Alexander Jager, Chair, Forum of Incident Response and Security Teams

Table of Contents

Vision

FIRST aspires to bring together incident response and security teams from every country across the world to ensure a safe internet for all.

An effective response is a global task, mirroring the global nature of the internet. Based on a peer-to-peer network governance model, Computer Security Incident Response Teams (CSIRTs), Product Security Incident Response Teams (PSIRTs), and independent security researchers work together to limit the damage of security incidents. This response requires a high level of trust. FIRST fosters trust-building among members through a variety of activities. Incidents are not restricted to one cultural or political corner of the internet, nor do they respect borders or boundaries. FIRST thus promotes inclusiveness, inviting membership from all geographic and cultural regions.

FIRST Mission

1. Global Coordination - You can always find the team and information you need.

> *FIRST provides platforms, means, and tools for incident responders to always find the right partner and to collaborate efficiently. This implies that FIRST's reach is global. We aspire to have members from every country and culture.*

2. Global Language - Incident responders around the world speak the same language and understand each other's intents and methods.

> *During an incident, it is important that people have a common understanding and enough maturity to react in a fast and efficient manner. FIRST supports teams through training opportunities to grow and mature. FIRST also supports initiatives to develop common means of data transfer to enable machine-to-machine communication.*

3. Policy and Governance - Make sure others understand what we do and enable us rather than limit us.

> *FIRST members do not work in isolation but are part of a larger system. FIRST engages with relevant stakeholders in technical and non-technical communities to ensure teams can work in an environment conducive to their goals.*

This Annual Report period has been incredibly challenging. Global events have unfolded, and sanctions have followed. FIRST strongly believes that our industry must operate in an inclusive environment, building trust at the technical layer where we work.

Read more on our website.

Organizational Update

FIRST remembers 2021 for the impact that the pandemic had on our in-person activities; however, we were still able to move forward with several effective organizational activities:

We successfully integrated the Industry Consortium for Advancement of Security on the Internet (ICASI) into FIRST. Established in 2008, ICASI's purpose was to strengthen the global security landscape by driving excellence and innovation in security response practices, facilitating collaboration among members to analyze, mitigate, and resolve multi-stakeholder, global security challenges. This role will continue as part of the existing ***FIRST PSIRT SIG***, expanding and improving the community's ability to respond to vulnerabilities across multiple vendors.

We became founding members of the ***Nonprofit Cyber coalition***. This coalition of implementation-focused cybersecurity nonprofits was established to collaborate, work together on projects, voluntarily align activities to minimize duplication, increase mutual support, and link the community to key stake-holders with a shared communication channel.

In addition, we hired two new members of staff. FIRST has grown in size over the years; it took 24 years to get to 312 full members, and it has taken us a further seven years to double that to over 627 full members today. More external organizations are requesting that we partner with or support their activities. We are conducting more activities online now and in person, which needs a more proactive and reactive operational team to respond and take action in real-time. The world we live in has grown more complex. So in response to this complexity, we created two new roles - a Director of IT & Security and a Director of Community and Capacity Building.

Dave Schwartzburg successfully applied for Director of IT & Security and started in early March 2022. Dave is well known in the FIRST community, having served on the board and as Chair. Dave stepped down from the board when he accepted this role.

The second role is Director of Community and Capacity Building. Increased capacity building is consid-ered one of the pillars of mitigating the increasingly severe effects of cybercrime or malicious state operations. For example, the 2021 UN GGE consensus report calls for states to engage in capacity building and explicitly calls for creating CERTs. The board decided that FIRST should hire a community and capacity building manager (CCBM) responsible for all FIRST activities in this area.

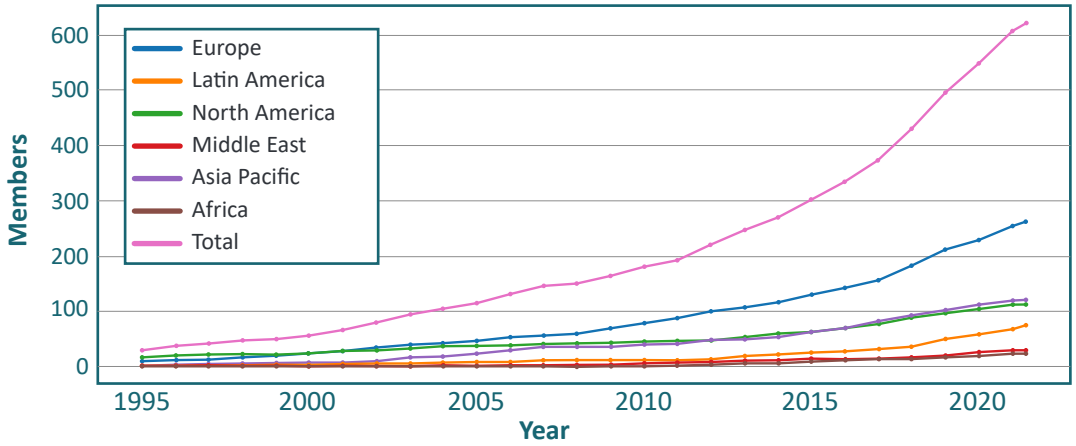
Klée Aiken, formally at CERT-NZ, successfully applied for this role, starting in mid-June 2022. Klée is also well known in the FIRST community through his work in the Pacific region and his time on the Advisory Board and Research Committee of the Global Forum on Cyber Expertise (GFCE).

Membership

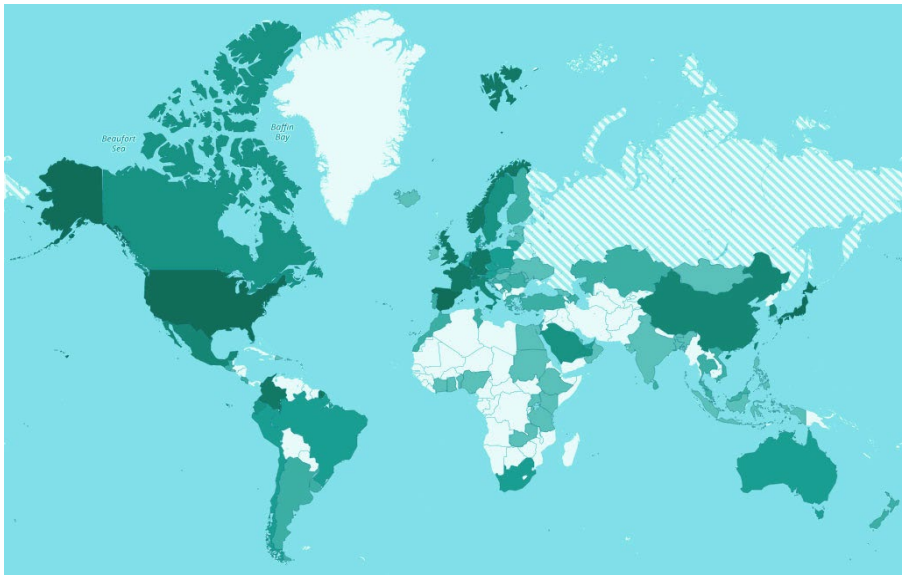
FIRST members are part of a network of computer security incident response and security teams that work together voluntarily to deal with computer security problems and their prevention. There are two types of members:

- Full Members represent organizations who assist an information technology community or other defined constituency in preventing and handling computer security-related incidents.
- Liaison Members are individuals or representatives of organizations other than incident response or security teams with a legitimate interest in and value in FIRST.

Membership of FIRST continues to grow. As of June 2022, we have accepted 627 members from 100 countries.



Since our last Annual Report, FIRST has significantly enhanced the FIRST membership application process. We incorporated a baseline SIM3 assessment into the application process for teams and sponsors. A new online application form was designed and launched within the FIRST portal. We are developing training on the new process and form filling for applicants and sponsors, including a SIM3 training, which we will roll out during the FIRST Annual Conference in Dublin. Additionally, our teams have updated the Services list within the membership application, and we updated the team profiles of existing members to reflect the CSIRT and PSIRT Services Frameworks.



Fellowship

Established in 2013, the Suguru Yamaguchi Fellowship Program aims to integrate security teams in unrepresented countries or regions into the global incident response community. During the 2021-22 period, FIRST chose Gambia Computer Security and Incident Response Team (gmCSIRT) and the Philippines National Computer Emergency Response Team (CERT-PH) to join the Program.

In early 2022, the FIRST Membership Committee developed a Mentorship pilot program for our Fellows. The new program aims to facilitate the integration and engagement of new teams within the FIRST community and introduce FIRST Fellows to our relevant activities.

We launched the first phase of the pilot in early 2022, seeking support from experienced FIRST members to become volunteer mentors. We will launch the program's next step at the FIRST Annual Conference in June 2022, where we will match mentors with mentees. If the pilot is successful, we may expand the program to new members and other interested teams to help them get more involved in FIRST's activities.

Events

Since our last Annual Report, we have organized eight events, three of them in person. These events ranged from a virtual FIRST Annual Conference previous summer to in-person Technical Colloquiums and a Symposium this year.

We still had many challenges in this period due to the global spread of COVID-19, as have many other organizations, but when we could, and in countries that opened up first, we held our events face-to-face with health precautions in place. Most of our events remained virtual, and our events team worked hard to make these as interactive as possible. The virtual events, including our Annual Conference, allowed a wider audience of incident response and security teams worldwide to participate in our events.

This year we were delighted to host our first in-person events for two years in Colombia, Norway, and the Netherlands. Feedback was very positive, with attendees glad to meet face-to- face and network. We look forward to creating other live events that allow our incident response and security team industry to meet. We believe this is essential to building a global community that trusts each other.

The events we held were as follows:

- 2021 FIRST Conference (Virtual)
- Three virtual Technical Colloquiums, two of them in person in the Netherlands and Norway

- Four Regional Symposia, three virtual in African & Arab Regions, Latin America & Caribbean, and Europe, and one in-person in Latin America & Caribbean. We are also preparing to reactivate the Asia-Pacific Regional Symposium for October 2022.

LAC4 Conference

Norway Conference

Our goal during these events is to provide a valuable and informative program to our members and other incident response and security team attendees. These events could not have been made responsible without the support of many volunteers and sponsors.

Read more on our website ***here*** and ***here***.

Training & Education

FIRST continued to hold several operational and technical training activities at FIRST events during 2021-22 to ensure CSIRT teams were well trained, some of which were collaborations with Data-Centric Audit Protection. We also delivered training to the Organization of American States (OAS) members in their training project under the umbrella of the CSIRT Americas project for information sharing, automation, and orchestration.

Read more about our training and education program ***here***.

Hall of Fame

In 2021, FIRST introduced two outstanding individuals to the Incident Response Hall of Fame - Jeffrey J. Carpenter and Dan Kaminsky. Both have significantly contributed to FIRST and the global incident response community.

Jeffrey Carpenter has dedicated more than 30 years to improving the state of information security. In 1995, Jeffrey joined the CERT® Coordination Center at Carnegie Mellon University's Software Engineering Institute, initially as an incident response analyst, then managing more than 50 technical individuals five years later. He was instrumental in helping the US Department of Defense and the US Department of Homeland Security create teams to exchange incident information and indicators between government and critical infrastructure organizations. He also worked closely with the US Department of Homeland Security to form US-CERT, the national CSIRT for the United States.

Jeffrey helped many worldwide governments and regional organizations establish national incident response capabilities. He founded a successful annual conference for technical staff working for CSIRTs with national responsibility to promote collaboration among these organizations. His active involvement in the incident response community has included presenting in various forums and serving on Forum of Incident Response and Security Teams (FIRST) committees and working groups. He currently is the Secureworks Senior Director of Incident Response Consulting and Threat Intelligence.

Dan Kaminsky (1979 – 2021) was a noted American security researcher - best known for finding a critical flaw in the Internet's Domain Name System (DNS) and leading what became the largest synchronized fix to the Internet infrastructure of all time in 2008. He was also known for being a great human - helping colleagues, friends, and community members attend events, working on many health apps, assisting color-blind people, hearing aid technology and telemedicine, and fighting as a privacy rights advocate. His ethos was to do things because they were the right thing, not because they would elicit financial gain.

Dan was Co-Founder and Chief Scientist of WhiteOps (recently renamed Human). He spent his career advising several Fortune 500 companies such as Cisco, Avaya, and Microsoft on their cybersecurity. In addition, Dan spent three years working with Microsoft on their Vista, Server 2008, and Windows 7 releases.

Many FIRST members are aware of Dan - some had the privilege of meeting and working with him. We will miss him and the energy, creativity, curiosity, and, above all, the fun he brought to our world.

The New York Times labeled him an "Internet security savior" - an honorific too often given but, in this case, very well deserved.

Read more about our Incident Response Hall of Fame ***here.***

Special Interest Groups

Special Interest Groups (SIGs) are a vital part of FIRST. Members come together to create new tools, define/refine standards, and learn from each other. While there were few face-to-face meetings over the last year, most SIGs kept driving their goals. FIRST gained three new SIGs this year: Women of First, Automation, and Multi-Stakeholder Ransomware SIGs.

- **CVSS SIG** plans to share a preview of CVSS v4.0 at the FIRST Annual Conference in Dublin.
- **EPSS** – This is this SIG's second year. The Group is actively improving the SIG, and website scores are updated weekly.
- **DNS SIG** – Actively working on mapping document.
- **Automation and Stakeholder SIG** – a new SIG with a few meetings undertaken. They are working to create deliverables and goals for the coming year.
- **CTI SIG** – Planning their SIG CTI Event.
- **PSIRT SIG** – Planning their fall PSIRT TC event for September 27-29, 2022, in Newton, PA, US.
- **Women of FIRST** – continues to meet and find ways to champion representation in the work force and field of study of incident response and security.
- **Academic & Metrics SIGs** – focuses on webinar-style meetings, usually for presenters to share works.

The following SIGs plan to meet at the Annual FIRST Conference in Dublin: **IEP**, **CTI**, **Red Team**, **Ethics**, **Automation**, **Vulnerability Coordination**, **VRDX**, **Malware Analysis**, **WoF**, **Security Lounge**, **Metrics**, **Academic**, **Cyber Insurance**, **TLP**, and **CVSS**.

With sufficient membership interest, new SIGs can be commenced and funded by FIRST. If you are interested in starting a SIG, please visit ***here***.

Standards

Many Special Interest Groups have been working on developing and improving standards this past year.

- The Traffic Light Protocol SIG (TLP-SIG) has worked on a new standard version. The Group has spent much time gathering feedback from the wider community and integrating it into the standard to keep it practical and straightforward.
- The DNS-Abuse SIG continues working on defining DNS abuse and has published a ***blog*** explaining why this is hard but important.
- The SIG associated with the CSIRT Framework Development actively worked at developing the standard further with regular meetings.
- In February, the EPSS SIG released its latest model, which the community positively received. EPSS complements the existing CVSS standard. FIRST is proud to contribute to tools that significantly help incident responders assess risks.
- The CVSS SIG continues to be improved. Members of the CVSS SIG are involved in the upcoming NIST standard 'Measuring the Common Vulnerability Scoring System Base Score Equation'.
- FIRST has contributed to the latest edition of ITU's "Guide to Developing a National Cybersecurity Strategy".

Read more on our website.

Diversity & Inclusion

Since the last Report, female members of FIRST have created a new Women of FIRST Special Interest Group to develop the success of FIRST further through increased female participation, leading to innovation in the field through diversity and inclusion.

Over the years, a range of informal and formal meetings culminated in a newly created SIG at the end of 2021 to develop a buddy program for security conference attendees and provide a forum for women to network and learn cybersecurity skills.

Women interested in joining this SIG can request to join the SIG ***here***. The Group will meet again at the FIRST Annual Conference in June.

Internet Governance & Policy

Since the last reporting period, two major United Nations bodies embarked on two initiatives related to our industry; the UN Open-Ended Working Group (OEWG) and the UN Ad Hoc Committee to Elaborate on a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes.

FIRST contributed to these initiatives by sharing our position on behalf of the incident response community. Board members represented FIRST at several meetings organized by the OEWG and the Ad-Hoc committee.

FIRST's position on the importance of ensuring that policy and governance must allow incident responders to continue to collaborate globally was reiterated.

It was stressed that policy and governance should help maintain the Internet's safety and security for all users and that an open and inclusive multi-stakeholder approach is essential for successful incident response.

Furthermore, agreeing with the 2021 OEWG consensus report, FIRST emphasizes that CSIRTs should be kept out of conflict and not be politicized. It follows that Incident response teams should be exempt from sanctions to be able to continue working together to protect their users.

ORF America

So far, we have made three inputs - one each on the general position of FIRST to the OEWG and the UN Ad Hoc committee and a specific contribution to the OEWG session on capacity building. FIRST emphasized that capacity is not only about knowledge but, equally important, about communities, i.e., the ability of CSIRTs to collaborate across organizations and countries.

Our CEO and board members participated in several other high profile events, including:

- A panel at the United Nations Institute of Disarmament Research (UNIDIR) flagship event, the 2021 ***Cyber Stability Conference***.
- A closed-door UNIDIR consultation on cyber operations about the war in Ukraine.
- 9th Sino-European dialogue, high-level diplomatic exchange between European and Chinese experts at the German ministry of foreign affairs.
- A panel on supply chain security and the role of incident response teams at the ***RSA Conference.***
- Two panels at the 2021 Internet Governance Forum. One on ***good cybersecurity practices and international mechanisms*** and some espionage operations' disastrous effects.
- A panel at the Swiss Internet Governance Forum on Hack Back.

As a result of our continuous work, the OEWG 2020-2021 acknowledged the importance of CERTs in its consensus report. There is consensus that incident responders play a crucial role in building trust among states and should be kept out of conflict.

Major Announcements & Press

Our annual communications activities are focused on delivering an integrated communications strategy to increase FIRST's global reach and awareness among incident responders worldwide and mitigate negative media coverage. Tactics executed included media relations, social media content about FIRST's activities, and keeping our members informed through a quarterly newsletter. FIRST shared four press releases during the last year and two blog posts:

- FIRST Technical Colloquium in the Netherlands – sees global experts converge in Amsterdam to share knowledge and inspire collaborations
- Meeting in person at the FIRST Oslo Technical Colloquium
- ICASI integrates into FIRST PSIRT SIG, bolstering the incident response and security team industry
- Jeffrey Carpenter and Dan Kaminsky were newly inducted into FIRST's Incident Response Hall of Fame
- FIRST appoints new Chair Dave Schwartzburg and welcomes five new Board of Directors
- Cybersecurity Nonprofits Form "Nonprofit Cyber" Coalition

FIRST was mentioned in publications from Canada to Japan - America Security Magazine, PC Magazine, Forensic Focus, SC Magazine, Security Magazine, Info Security Magazine, Helpnet Security, IT World Canada, Revista Sic, Tech Smart, ZDNet, Cloudcow, Techbeacon, Yahoo, and Wirefan. FIRST was also referred to by the Hong Kong government as a step towards global collaboration and cyber security defense.

Our quarterly newsletter emailed directly to our members has sustained a readership of nearly 400 from over 35 countries per issue and is well-read across the US, Europe, the Middle East, and the Asia Pacific.

Social media reach continues to increase.

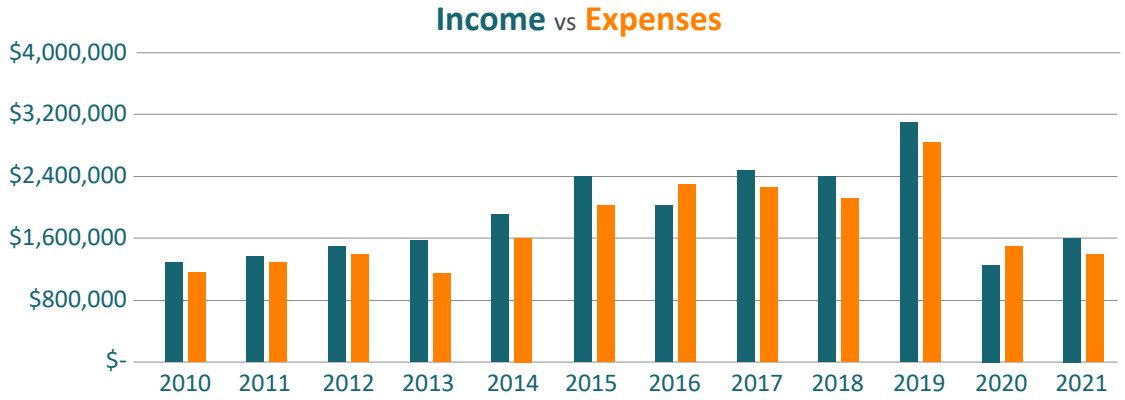
We saw a significant increase in followers across our social media channels in the past 12 months. The total number of followers is now at nearly 16,000, with over 2000 new followers and an aggregated global impression of 240,000 across FIRST social media channels - Facebook, Twitter, and LinkedIn.

Read more in our newsroom.

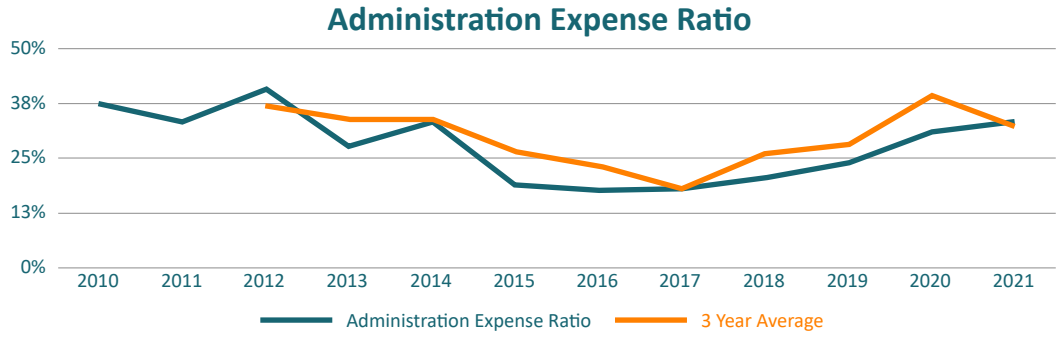
Financials

The global pandemic continued to impact the finances of FIRST through 2021. Again, in-person events were considered too risky throughout most of the year, significantly reducing registration fees and sponsorship agreements.

The board has initiated a review looking at options to reduce FIRST's reliance on events for income. Before the pandemic, FIRST used surplus from events to fund SIGs and other activities. As FIRST takes on long-term commitments related to our staff and other operational activities, we need to broaden our income to ensure we can meet these. We corrected last year's slight deficit into a small surplus through strong fiscal management by reducing expenses and increasing income for the year.



As a 501c3 organization, it's best practice to keep administrative costs below 25% of total expenses. As of 2020, we have been unable to hold many in-person events. Much of our administrative expenses are from long-term commitments related to support services and staff costs. These expenses caused the admin to total expenditure ratio to rise to approximately 32%. As stated in the last Annual Report, our ambition is to return to the former ratio as soon as possible.



FIRST commissioned a Finance Audit which took place in early 2022. We will report on these results during our Annual Conference in June 2022.

FIRST is a financially sound organization and a 501c3 nonprofit incorporated in North Carolina, USA. Detailed financial information is available through our members portal or provided to interested parties such as grantors and sponsors upon request.

You can find previous financial reports here.

Infrastructure

Over the past year, the infrastructure team has worked on several initiatives to optimize FIRST's services and operations for its members, staff, and volunteers. The following are some highlights:

- The membership application was updated and improved, including integrating the ***Open CSIRT Foundation SIM3 model***.
- The team has deployed Google Workspace for the Board of Directors, staff, and FIRST employees to provide enhanced email and calendaring services.
- A new ***Exploit Prediction Scoring System*** (EPSS) ***API*** was developed and made available publicly, significantly improving the ability to leverage the framework.
- We implemented the New Groups functionality, improving the ability of working groups, SIGs, and other informal FIRST groups to manage their members and related resources better. This allowed members and volunteers to apply to participate in various groups more easily.
- We integrated the event registration process with single sign-on as well as new checks to help protect FIRST from sanctions and compliance-related issues.
- The invoicing for FIRST member dues was successfully migrated to Quickbooks Payments, streamlining payment options and eliminating PCI compliance requirements.
- Access to the FIRST API was enhanced to support improved authentication, discontinuing the use of X.509.
- The ICASI acquisition was completed, and **icasi.org** is now managed by FIRST and redirects to the ***FIRST website***.
- There has been a continued focus on implementing best practices, including DNSSEC & CAA.
- Planning is underway to migrate in-house services from the existing hosting platform to AWS.

https://www.first.org
first-sec@first.org

Forum of Incident Response and Security Teams
2500 Regency Parkway, Cary, North Carolina, 27518
United States of America