FIRST CORE:
Impact Vision

FIRST CORE seeks to share the expertise and insights of the global incident response community to help improve security, together. Below you will find a short introduction to some proposed initiatives the FIRST Community & Capacity Building (CCB) team seeks to activate through CORE.

The design and delivery of the FIRST CORE initiatives are informed by the needs, priorities, and aspirations of partners on-the-ground and programming is intentionally designed to be highly flexible and responsive. The ultimate ambition and scope of the activities delivered under CORE will be determined by the amount of funding available.

Enabled by CORE, the FIRST Community and Capacity Building Program will continue to develop tailored initiatives to address needs, priorities, and ambitions of the incident response community. CORE will also explore where small grants might have the opportunity to catalyze impactful community driven initiatives, including kick start support for the establishment of local cybersecurity communities of practice or to enable information sharing networks.

The CORE program enables initiatives and support under three buckets:

- **Capacity Building Initiatives**: using FIRST's unique, world-spanning community of 800+ members, your support is primed to build up key skills of cybersecurity professionals that help keep our networks and societies safe. These initiatives will create structural capacities that can deliver new trainings on demand, with our Regional Liaison programme as a flagship example, as well as dedicated projects meant to close real cybersecurity gaps.
- **Community Building Initiatives**: while trainings help our professional networks keep one step ahead of threat actors, what most in the FIRST community profess to want is the sense and benefits of the community that they have joined. FIRST organizes dozens of global, regional and topical meetings and workshops annually, which, sadly, a lot of our members from disadvantaged communities are unable to

fully benefit from. Moreover, with direct aid becoming scarcer, a lot of inspired initiatives brought to FIRST through the Global South members of our Special Interest Groups (SIGs) are forced to stay on the cutting room floor. Your support, as a CORE funder, will help us even this playing field through fellowships and helping bring world-beating SIG ideas to light.

- Back-of-House Support, Contingency, and Continuity (BCC): FIRST is a lean organization that counts on drive and initiative for the most part, but it also relies on a small team of dedicated professionals to maintain the events, platforms and projects our community benefits from. Accordingly, a percentage of your donation helps us maintain this high level of support.

For more information on current FIRST Community and Capacity Building Initiatives or to learn more about the type of work that FIRST CORE seeks to enable, reach out to the team at CCB@first.org.

Capacity Building Initiatives

FIRST Regional Liaison Initiative

The FIRST Regional Liaison Program seeks to establish a network of dedicated technical practitioners to support the development of incident response teams, regional information sharing networks, and local communities of practice in regions underrepresented in the global incident response community.

Each Regional Liaison will work with incident response teams and relevant partners in their region across a menu of activities, including:

- Information and good practice sharing and development;
- Formal and informal mentorship and advisory support;
- Delivery of localized incident response training;
- Development of regional information sharing networks;
- Community outreach, development, and engagement; and
- Peer-to-peer capacity building across the region and with global partners.

The Liaisons function as trusted members of their regional incident response communities, capable of providing ongoing support with the depth of local understanding necessary to deliver impact. The Liaisons are experienced incident response practitioners positioned to provide direct advice, mentorship, and training as well as to act as a bridge between the regional community and the global incident response community.

FIRST currently has a dedicated Africa Regional Liaisons based inKenya as well as coverage in the Western Balkans and the Pacific. Further Liaison roles being prioritized include Latin America & the Caribbean, Asia-Pacific, and Western Balkans and Central Asia.

FIRST A4 Initiative

Effective incident response extends well beyond handling incidents as they arise. One of the most persistent challenges for teams across every context — regardless of country or capacity — is translating available threat intelligence into meaningful preventative action: getting good information, processing it effectively, and communicating it in a way that stakeholders read and act upon. The FIRST A4 (Actioning Alerts and Advisories) initiative was developed to address this challenge directly.

A4 approaches the problem in two complementary parts. The first is technical: helping teams understand where to source threat intelligence, how to parse and integrate it into their existing systems, and how to assess its relevance to their country or sector. FIRST works with technical experts — including practitioners closely associated with tools that teams already use, such as Shadowserver and IntelMQ — to provide hands-on support that is directly applicable to each team's current infrastructure. The second part is communication: working with teams to identify their constituents, assess the effectiveness of existing outreach, and develop or refine advisory outputs that are genuinely fit for purpose. FIRST's communications experts guide teams through a series of workshops, bringing in external stakeholders and, where relevant, communications staff from wider ministry or agency teams.

Rather than prescribing a rigid agenda, A4 is designed to be adaptive — each team receives a version of the programme tailored to their specific needs and context. The four core workstreams are:

- Supporting access to no-cost resources — such as Shadowserver — as well as linking teams with international experts in the fields of threat intelligence and communication;
- Supporting teams to improve their good practice guides and advisories through the sharing of multi-phase mitigation, remediation, prevention, and intervention playbooks;
- Providing in-person training and meetings to develop localised and contextual resources for each country, and encouraging outreach to different sectors such as banking, government, and academia; and
- Producing resource and playbook outputs with specific considerations for incident response team outreach and engagement with civil society organisations and vulnerable groups.

A dedicated FIRST Training and Mentorship Fund

The FIRST community of trainers and mentors provide an invaluable resource for teams around the world to collaborate, develop and refine services, gain new skills, and improve the way they work. A FIRST training and mentorship fund would help support the development of FIRST training materials and trainers and to subsidize training and mentorship engagement costs where needed.

The trainings that experts within the FIRST community can offer span the full spectrum of incident response practice, with technical courses covering areas such as network traffic analysis, malware analysis and reverse engineering, vulnerability management, and the use of threat intelligence platforms and sharing standards. If a best practice exists, our community has it.

This also makes mentorships and train-the-trainer (T3) initiatives, already piloted by FIRST across Africa, so valuable. We build mentorships through our trainings, recognize holders of best practice and pair them with those best able to adopt these skills instead of dropping in established experts from regions with practices inapplicable to the needs of prospective mentees.

This fund is intended to be paired with the growing FIRST network of regional liaisons, who are best positioned both to identify and shape training opportunities within their regional communities, and to identify prospective mentors and T3 leads.

Community Building Initiatives

Enhanced Fellowship Program

Named in honour of the late Dr. Suguru Yamaguchi — a founding member of JPCERT/CC, former FIRST Board member, and the initiator of the Fellowship — the Suguru Yamaguchi (SY) Fellowship Program is a four-year program designed to support new and growing national-level incident response teams to engage with the global incident response community. Fellowship funding is currently focused on supporting attendance at the FIRST Annual Conference, alongside reduced membership costs and access to community mentors.

The SY Fellowship cohort reflects the diversity of the global incident response community. Current and alumni teams span Sub-Saharan Africa, the Asia-Pacific, Latin America and the Caribbean, Europe and Central Asia. Collectively, fellowship teams bring expertise spanning national CSIRT coordination, sector-specific incident response (government, academia, and private networks), and all-of-government cyber resilience.

Enhanced CORE funding for this work stream would allow for a broader range of capacity building opportunities throughout the year, including access to FIRST training courses, participation in Regional Symposiums, and the exploration of staff secondment opportunities - significantly deepening the value of the fellowship experience beyond the Annual Conference.

FIRST SIG Fund

The FIRST network of Special Interest Groups (SIGs) are a central component of the FIRST community, providing a forum where incident response practitioners can discuss topics of common interest; develop and share good practice and lessons learned; collaborate on standards and trainings; and address common challenges. Nearly three dozen of these Groups exist at the moment, with their numbers only scheduled to rise with time, as their formation is not subject to top-down decisions by FIRST leadership – rather, any members of our community, recognizing a topic essential for the work of their security team or organization, can establish a SIG with other like-minded members. In a testament to this organic nature, even across FIRST's decades of work, over 90% of SIGs remain fully and consistently active. In the course of its work, the SIGs consistently approach FIRST and the CCB team with ideas for collaboration that, if appropriately resourced, could help alleviate chronic issues that can disrupt effective responses to cyber incidents, ranging from better handling staff attrition through the Human Factors SIG to learning platform and training support across groups. The FIRST Special Interest Groups allow for coordination and knowledge sharing through informal conversation, relationship building, and training. Additional funding allows groups to explore new ideas and initiatives of interest.

Under this initiative, FIRST will create a formal process through which SIGs are able to submit proposals to tap the newly created SIG Fund. Initiatives will be chosen based on their ability to help their community and capacity building efforts, including for the creation or updating of training materials, e-learning resources, good practice documents, and other initiatives to advance the work of the SIG and global incident response community.

Women of FIRST SIG Support

As part of FIRST's commitment to diversity and inclusion, a specific fund will be designated to support the work of the Women of FIRST (WoF) SIG. The WoF SIG has initiated a number of programs, including an ongoing webinar series, and are exploring other potential efforts including mentorship and fellowships. Any work funded through this support will be designed and delivered with guidance from the WoF SIG.

Back-of-House Support, Contingency, and Continuity (BCC)

Delivery of CORE programming requires strong back-of-house and administrative support to enable successful initiatives. CORE Back-of-House support funding will be limited to no more than 20% of CORE funding. A portion of CORE funding will also be held in reserve as contingency for ongoing CCB activities and to cover continuity costs to allow a soft landing should project based grant funding expire.