Project Summary

SDAIA addresses a critical need for security solutions for Science DMZ networks, and further represents a strategic value of establishing an intelligence foothold that will benefit our national cyberinfrastructure through greater situational awareness. Secondly, we aim to provide the cybersecurity research community with a rich, real-world intelligence source upon which to test their theories, tools, and techniques. Our efforts are in response to recent NSF investment and efforts by ESnet that have spurred a rapid growth of open high performance networks or so-called Science DMZ deployments. Science DMZs support big data and access to high-performance computation through very high bandwidth networks in an open environment that presents new challenges to the traditional university security stance.

Science DMZs are positioned in front of campus firewalls to enhance performance and this translates into the need for new security solutions. Crucially it must be done in a way that is simple to deploy and affordable on a higher education budget. The SDAIA project will provide a holistic approach that will address the special Science DMZ architecture through a new kind of virtual security appliance that will benefit from external, shared intelligence to protect the site, and further provide intelligence to the wider community of both DMZ operators and cybersecurity researchers. This appliance will leverage existing technologies; be easy to deploy, configure, and maintain; integrate with common Science DMZ services, and be built upon free and open source software for affordability and flexibility. In addition, our solution will be developed with an awareness of software defined networking (SDN) to ensure that our approach can readily integrate with emerging SDN-based networks.

Our proposed project will integrate efforts from both NSF and DoE to advance the security infrastructure available for Science DMZs, which enable scientific research from astronomy to zoology. The SDAIA project will actively promote sharing of intelligence among science DMZ participants as well as with the national scale XSEDE cyberinfrastructure and any other projects or organizations that wish to participate. Beyond meeting the security needs of campus-based DMZs, the SDAIA project will lay the foundation for an intelligence sharing infrastructure that will provide a significant benefit to the cybersecurity research community, making possible the collection, annotation, and open distribution of a national scale security intelligence for security research. This intelligence will highlight and support cybersecurity research for a new wave of open networks that rely more on monitoring and attack response than they do on static firewalls and port blocking. Further by making the intelligence feeds available to security researchers we envision novel ways to digest and utilize these feeds for such things as intelligence analytics, attack type characterizations and frequencies to name a few.

In addition to providing a packaged security monitoring/response system for Science DMZ operators, our project will raise the bar of security expertise within that community by making annotated intelligence available, which may include actions taken by sites reporting the intelligence. Through this and through the formation of the intelligence sharing network our work will serve to bring together Science DMZ practitioners to share not just raw intelligence but also their deeper individual and collective experiences including what they are seeing and the success or failures of the controls they implemented. Beyond that, cybersecurity researchers will have an active and near real-time way to collect intelligence from this network on a national scale. This data will be annotated with additional details to provide researchers a deeper view into what is actually going on and enabling research that is difficult at best without real-world intelligence feeds.