Security Engineering & Management
U.S. Nuclear Regulatory Commission
Past Performance

Provided below is a summary of security-related services that have been and/or currently are being provided to the Nuclear Regulatory Commission (NRC) since 2012.

Security Configuration and Management Services

Experience: In support of the NRC, G2SF is responsible for the Cyber Security Service function, including the Security Architect key position. The NRC has a national presence and the security service includes all aspects of operational security. The service includes layer 3 and layer 7 firewalls (Next Generation), MTIPS management and coordination, circuit monitoring, Antivirus and Malware, sandboxing technology, vulnerability and compliance scanning, email filtering, web proxies, WAN optimization and encryption, centralized log management, SIEM, network access control and wireless (802.11) control and defense. At the NRC, G2SF currently supports Cisco ASA firewalls, Palo Alto firewalls, Palo Alto Wildfire appliance, Cisco IronPort Email Appliances, Trustwave malware scanners, Tenable Security Center and Nessus scanners, Splunk, Symantec Endpoint Protection, McAfee ePO, IBM QRadar, What's Up Gold, Riverbed, BlueCoat web proxies, ForeScout CounterACT NAC, and Infoblox DNS/DNSSEC.

Capabilities: G2SF has directly applicable experience preparing and protecting agencies against security threats with innovative, resilient, actionable cybersecurity architecture, design, implementation and management services. We have the experience to optimize and enhance security tools across the enterprise to effectively leverage existing assets and licenses. We help implement solutions that prioritize, repurpose, and reconfigure current tools and reduce the need to acquire new ones. To do this G2SF provides:

- Certified experts with in-depth knowledge of a wide range of technologies
- Repeatable processes that consider enterprise system mission, resources, and asset criticality
- Remediation planning that addresses potential vulnerabilities, mitigating factors and impact on critical assets
- Implementation support based on well-documented security plans and training of security personnel across a wide range of roles and responsibilities

G2SF assists our customers in identifying, defending and remediating security risks. We assist in compartmentalizing critical functions to reduce the impact of a security event by limiting exposure of sensitive data. We place sensors and tailor security solutions to ensure complete on-press security coverage and isolate network traffic to limit collateral damage in the event of a breach. We help place, configure and deploy deep security solutions for:

- Large networks
- Mobile platforms
- Cloud solutions
- Wireless networks

We work with a wide range of security architecture tools, including:

- Network Access Control (NAC)
- Public Key Infrastructure (PKI)
- Multi-factor Authentication
- Host-based security tools
- Vulnerability management tools
- Configuration management tools
- Hardware and software management tools
- Networking devices
- Perimeter defense appliances such as Firewalls, IDS/IPS, and web proxies
- Traffic inspection

Security Weakness and Threat Detection

Experience: At the NRC, G2SF's security service is responsible for the agency's national presence. G2SF performs and participates in continuous internal and external cyber security audits and tests. NSA, DHS, GAO, GSA and others have all conducted security audits. We work with our federal counterparts to address the resulting Plan of Actions and Milestones (POAMs). In both preparatory and remediation actions, the G2SF team has evaluated and designed products and techniques to keep up with current and potential weaknesses. By following the National Institute of Standards and Technology (NIST) Risk Management Framework and the Protect, Detect and Correct closed feedback loop, after-action plans and standard operating procedures are created or improved. G2SF operates a weekly security roadmap projects meeting to facilitate federal and contractor oversight and input into the tools and techniques used. The roadmap prioritizes risk and funding to deliver the right tools and techniques the agency needs now and, in the future, with full ownership by both the contractor and the government.

External scanning includes Qualys, WebInspect and DHS's weekly Cyber Hygiene Report. The commission's Office of the Inspector General (OIG) and others occasionally engage external Red Teams to probe and measure the security posture. Internally, the primary tools for analyzing security strength are Tenable Security Center and Splunk. Microsoft's SCCM and ForeScout's CounterACT are also used to give patching compliance statistics. NRC is currently implementing the DHS provided Continuous Diagnostics and Mitigation (CDM) components and G2SF is the primary onsite integrator of the toolsets. The CDM tools leverage G2SF's existing tools to gather security posture information and allow the commission's data to be transmitted, base-lined and evaluated in dashboards at DHS.

Capabilities: From a security perspective, G2SF takes a holistic approach to analyzing networks and systems using well recognized standards and industry best practices while taking into consideration agency goals. G2SF compares existing security management practices against these best practices and standards to identify network/system weaknesses to ensure compliance to federal standards and agency policies. G2SF has experience:

- Providing cyber security subject matter experts that are cross-trained in multiple compliance frameworks
- Conducting security assessments to identify and resolve system and network vulnerabilities and closing the gaps between current security operations and operations based on standards and best practices
- Proactively advising clients regarding risks and ensuring that cybersecurity strategies are aligned with the mission
- Looking beyond compliance and toward developing and executing security plans/roadmaps to further strengthen the overall security posture at both the system and agency level

Security Operations Center (SOC) Management

Experience: At the US NRC, G2SF's security service includes operating a 24x7x365 SOC. Occupying the key position of Security Operations Center (SOC) and Compliance Manager, G2SF personnel currently provide management, staff, and oversight of the Security Operations Center (SOC), the Information Assurance (IA) function, and the Identity, Credential and Access Management (ICAM) teams. The G2SF security team has considerable experience executing, managing and validating security/IA requirements in all aspects of Federal, Military and Commercial security programs. G2SF's NRC security personnel have worked with DIACAP, National Information Assurance Certification and Accreditation (NIACAP), DoD Risk Management Framework (RMF), Federal Information Security Management Act (FISMA), Director of Central Intelligence Directives (DCID) 6/3 (and its replacement Intelligence Community Directive (ICD) 503) and are actively addressing the changes instituted in the recently released National Institute of Standards and Technology (NIST) 800-53 revision 4. The G2SF security team has taken a practical, best of breed approach to working NIST 800-53 revision 4 requirements and has integrated the standards into new and emerging NRC projects and implemented the appropriate controls to fully secure the technology. G2SF has routinely evaluated the existing controls for NRC systems, allowing for a cycle of continual improvement before issues become findings or vulnerabilities. G2SF is also responsible for coordinating with commercial providers, including the United States Computer Emergency Readiness Team (USCERT), as well as multiple Operations and Maintenance (O&M) contractors who provide comprehensive security services for the NRC. Employing highly qualified staff, the G2SF-managed SOC supports a broad security product suite that provides daily protection from both external and internal threats. This support includes auditing, data loss prevention, spillages, and investigations. In addition, the G2SF-managed SOC is responsible for transforming the NRC legacy enterprise vulnerability and compliance scanning system. As one of the key components in the Department of Homeland Security Continuous Diagnostics and Mitigation program for vulnerability and compliance scanning, the system is deployed as virtual machines and can be scaled on demand to meet new requirements from internal and external stakeholders. This tool is used by G2SF for daily activities, but also by Agency Information System Security Officers (ISSO) and the Independent Verification and Validation (IV&V) contractor. By implementing this system, all parties can access the same rules and results, thereby reducing rework and potential vulnerabilities The SOC is comprised of Tier1, 2 and 3 level analyst/engineers. Tier 1 analysts are trained in the standard operating procedures and are effective at triaging potential security incidents. This tier often deals with simple email and web proxy events. They also will initiate antivirus scans on computers that have received spear phishing or suspected malware. They use off-network malware PCs and submit suspect files to sandbox engines. Tier 2 analysts have more comprehensive knowledge of the commission's national cyber landscape and can evaluate more deeply if threats are real. Tier 2 analysts are fully trained in QRadar and Splunk's SIEM to look for off-baseline activities and evaluate forensic data. Tier 3 analysts are extensively certified and trained and participate in conferences, user groups and security forums to keep their skills current.

As part of the Homeland Security Presidential Directive 12 (HSPD-12), G2SF led the effort for the establishment of mandatory smartcard logon for privileged and un-privileged accounts. G2SF engineers conducted a series of activities with key NRC stakeholders to identify, define, document, and verify the architectural, design, functional, and performance requirements. These requirements were used by the NRC to select G2SF's recommended interim solution while application and infrastructure issues were resolved. This approach led to the migration of users, workstations and servers into a compliant state. Privileged accounts were migrated to a Role Based Access Control (RBAC) model to maintain Tier-0 (Domain/Enterprise Admin), Tier-1 (Server), and Tier-2 (Workstation) separation/isolation. Tier-0 and Tier-2 accounts are now 100% User Based Enforcement (UBE).

Tier 1 are UBE exempt only for the duration of their documented use case(s). This required integration with NRC's Identity, Credential and Access Management (ICAM) system to ensure Active Directory user accounts became and remains Personal Identity Verification (PIV) capable. This required creating/updating GPO objects, designing Active Directory groups, and developing a policy/procedure

for PIV card use cases (lost or forgotten badge temporary access) and RBAC accounts. To support the Cyber Sprint initiative and to follow the established requirements analysis process, G2SF engineers accelerated and successfully completed the Microsoft Active Directory upgrade from 2003 to 2012 R2. This entailed following a strict schedule based on federal directive to obtain approval for the NRC's use of Windows 2012 R2 following DISA STIGs until NRC standards were finalized.

A recent Security Roadmap COTS study led by G2SF on next generation antivirus compared five software packages with zero day malware in a G2SF's test lab. Palo Alto Traps, Cylance, Invincea, SentinelOne, and Symantec 12 were installed on the NRC's standard workstation image. Each had its pros and cons, with the Symantec 12 (old generation antivirus) doing the worst. The final results showed Invincea the clear winner based on NRC and G2SF's requirements matrix and the commission is currently reprioritizing funds and resources to initiate a full rollout. This product will reduce the number of rebuild actions that are needed currently as remediation actions.

Capabilities: As identified in the experience section above, G2SF provides comprehensive, end-to-end SOC security solutions. Our staff hold multiple industry certifications, including GPEN, GCIH, GWAPT, CREST CCT, MCSE, RHCT, OSCP, OSCE, NSA IAM/IEM, CEH, PMP, ITIL and CISSP. G2SF's security professionals are highly experienced with a wide variety of technologies and can perform competently in almost any environment.

Network Cryptography Services

Experience: At the US NRC, G2SF designs, establishes and maintains multiple virtual private network (VPN) connections. Site-to-site VPN connections are accomplished with either Cisco ASA concentrators (being phased out) or Palo Alto firewalls. G2SF also runs the Citrix NetScaler SSL VPN appliances and client software on mobile workstations. Additionally, by operating perimeter firewalls and proxies, the G2SF team ensures there is no unapproved VPN activity.

Capabilities: G2SF understands organizations are demanding increasingly larger amounts of bandwidth and an extremely reliable set of converged VPN services to deliver a suite of voice, video, and business-critical data applications to users with the desired level of performance and quality of service (QoS). Today's IP VPNs are based on multiprotocol label switching (MPLS) technology. We actively manage site-to-site connections, with our MPLS service provider managing the end-to-end network. We have deployed VPNs in a number of ways, all with FIPS 140-2 compliant cyphers and algorithms:

- Network-based IP VPNs using the secure infrastructure of a single network provider
- Using client IPSec tunnel
- Using Secure Socket Layer (SSL)
- Virtual VPN – With the advent of software defined networks and virtualized data centers, virtual firewalls have had to mature. G2SF has tremendous experience with port trunking, vlan tagging, east-west traffic and maintaining separation of zones and workloads. Proving separation and preventing clan hopping are key goals that G2SF can display to auditors

As a technology agnostic solution provider, G2SF has the understanding, prior experience, and capability to design, implement and manage a VPN solution that meets the unique needs of the customer.

Type 1 Encryption of Classified Networks

Experience: G2SF resources are NSA-trained COMSEC custodians who have performed work on SIPRNET and JWICS. The G2SF team has recent experience working with both NSA and the Pentagon Connection Office to establish SIPR circuits with Type 1 encryption. We have experience ordering COMSEC equipment from Raytheon and acquiring keys through our COMSEC account with the

NSA management team. G2SF is highly skilled at deploying cryptographic equipment. For example, when we receive the encryption keys, they are loaded and then we work with our government counterpart to configure the encrypted connection by synchronizing the keys. Once the keys are loaded, the system then becomes classified and we keep all COMSEC equipment in a secure area, separated from other components of our SIPR network.

Capabilities: Our overall capabilities range from acquiring, installing, and configuring the Type 1 encryption equipment and establishing the encrypted connection to physically securing the equipment and data lines in accordance with federal and agency regulations and policies.

Application and Database Server Security Services

Experience: G2SF participates in many C&A and ST&E activates at US NRC. The NRC does not have an IATC system in place but utilizes essentially the same steps when bringing on new projects or technologies onto the network. The Tenable Security Center is the principle tool used to perform DISA STIG compliance scanning on applications and databases. The results of the scans are used by either the configuration control board or Designated Accrediting Authority (DAA) to make risk-based decisions on authority to operate or connect. G2SF operates and maintains the Tenable system at the NRC.

As part of our Operations and Maintenance (O&M) responsibilities for the USMC ITSM tool suite, G2SF was tasked with providing security requirements identification, analysis, allocation, and tracking support utilizing Defense Information Assurance Certification and Accreditation Process (DIACAP). These efforts also included assisting the Government in retaining the Authority to Operate (ATO) through all USMC ITSM suite upgrades and capability improvements, as well as developing and editing accreditation packages for the training, pre-production, and production environments. In support of these requirements, G2SF System Engineers and IA specialists created and maintained a (POAMs) for five (5) Remedy environments and remediated or mitigated findings discovered during Assured Compliance Assessment Solution (ACAS) and Security Content Automation Protocol (SCAP) scans.

Capabilities: G2SF understands that organizations are facing exponential increases in the amount of information and data that they need to continuously track, manage, and protect to ensure mission success and continuity of operations. Most attacks remain focused on denial of service. However, sometimes hackers target the database because that is where sensitive information resides. Our staff understands that with so much at risk, we share a responsibility with our clients to secure the databases. We frequently assume the role of stewards of the data to ensure that operations are not threatened. In light of that responsibility, we typically work with our customers to implement the following best practices:

- Separate the database and webservers
- Encrypt stored files and backups
- Deploy web applications firewalls
- Keep patches current
- Enable database security controls
- Monitor database connections and block connections when the data stream varies from protocol or expected behavior.
- Ensure OS and databases are built in accordance with DISA STIGs and industry best practices

Anti-Virus Scanning Scope

Experience: G2SF operates all versions of antivirus and malware scanning software at the US NRC. In the current threat landscape, it has proven useful to operate redundant products in the antivirus and malware area because what one tool doesn't see, another often does. Symantec Endpoint Protection 12 is

the primary tool used by G2SF on workstations and servers. A change request has just been submitted to migrate that instance to Symantec 14. Recent briefings from Symantec make claims that they are moving from the traditional signature model to more of a behavior base model. On perimeter gateways, Sophos, Palo Alto antivirus and Wildfire are also used.

Capabilities: G2SF staff have the ability and experience to implement and operate a wide variety of different antivirus software solutions as part of an overall agency security solution.

Security Architecture and Model

Experience: At the NRC, G2SF employs both the primary security architect and network architect position for the commission. It is a contract requirement to document and maintain network and security architectures. This includes the perimeter DMZs as well as WAN IDS/IPS points and datacenter zoning. These areas are depicted in their respective management platforms as well as Visio drawings, PDFs and other large format visuals. The G2SF team creates and maintains all written material used in the systems' SSPs based on the NIST 800-53 rev4. The systems that G2SF operate and document are operated at a security categorization of HIGH and, therefore, have all of the control families fully documented.

Capabilities: G2SF staff have the experience and capabilities to design, build, implement and document network security architectures. Our design methodology considers all aspects of network security and its integration with the core network infrastructure. Using an in-depth, architectural approach based on industry standards, G2SF security experts develop a multilayer defense against directed attacks from hackers and indiscriminate attacks from viruses, worms, as well as insider and outsider threats. We utilize an architectural approach that is built to last yet can evolve over time to support the deployment of new technologies. We define a standardized and common set of security solutions, policies, and practices that can be replicated, thus reducing complexity and cost. We understand that often, simpler is better and this results in an increase in efficiency and visibility in diagnostic analysis. Our approach is composed of two primary services:

- Security Design Assessment – Assess the existing network security design to identify architecture, design, and implementation vulnerabilities and provide recommendations for building, improving, or reengineering the customer's network security design
- Security Design Development – Develop a strategy, plan, and detailed design for integrating enhanced and/or new security solutions into the network infrastructure

External Network Interface Services

Experience: At the NRC, the G2SF team operates all of the egress points of presence from the enterprise to the commercial MTIPS provider. At the perimeter, application aware firewalls and explicit proxies are used to protect and monitor web activities. Both the BlueCoat proxies and the Palo Alto firewalls are used to intercept/decrypt SSL traffic and inspect for malware, data loss (DLP), VPN tunneling, inappropriate sites or content, and command and control traffic. The G2SF-operated SOC also maintains custom signatures on the firewalls and proxies based on commission-specific threats and trends. White and black lists are maintained to further define and refine approved sites and services. The data from these tools are often used in employee training and counseling and sometimes in legal proceedings.

Capabilities: As part of our overall security offering, G2SF has the experience and ability to manage a variety of different technologies to provide an out-of-band management port (MGT) to perform the firewall administration functions, as previously referenced. Using the MGT port, we separate the management functions from the data processing functions of the firewall, safeguarding access and enhancing performance. We typically use a web interface to perform all initial configuration tasks from

the MGT port, even when planning to use an in-band port for managing devices going forward. Determining the firewall management strategy will impact malware inspection (sandboxing technologies), URL and HTTP/HTTPS filtering. We protect the MGT port with two factor authentication and User-ID functions to assure the security posture of the device. We have helped multiple civilian, DoD, and Intelligence Community customers develop and implement their firewall management strategy for the management of external interfaces, including DMZs, Datacenters and WAN egress points.

Demilitarized Zone (DMZ) Services

Experience: At the NRC, G2SF has been operating a comprehensive enterprise security service for six years. During that time, all aspects of the DMZs (demilitarized zones) have been refreshed and redesigned. The original DMZs were comprised of Cisco ASA layer 3 type firewalls. Those DMZs produced no useful IPS/IDS information to protect the NRC. The logs were sent to QRadar and centralized logging systems, but that was often too little, too late. G2SF ripped and replaced all switches, routers and firewalls related to the DMZs. Now all traffic to and from DMZs are fully inspected and evaluated by application filters that weed out malicious traffic. Friend or foe decisions are made immediately and automatically by the firewalls. At the same time all executable files that traverse the DMZs is sent to an onsite Palo Alto Wildfire malware sandbox for evaluation. G2SF makes recommendations to the NRC about OS versions, virtualization, protection technologies, domains membership, authentication and other DMZ-related topics on an ongoing basis. All designs and as-built documentation are provided to the NRC as contract deliverables.

Capabilities: G2SF engineers understand a DMZ or a perimeter network is a physical or logical sub-network that separates an internal local area network (LAN) from other untrusted networks, typically the Internet. External-facing servers, resources and services are located in the DMZ so they are accessible from the Internet, but the rest of the internal LAN remains unreachable. This provides an additional layer of security to the LAN as it restricts the ability of hackers to directly access internal servers and data. G2SF staff has experience architecting services that are placed within the DMZ based on federal and agency policies. These services include Web browsing, email, DNS, FTP, and VoIP. We understand that systems running these services in the DMZ are reachable by hackers and our staff is experienced in hardening them to withstand constant attack.

Our staff is experienced in designing and evolving networks using a DMZ. This includes using single or dual firewalls. These can be expanded to create very complex architectures, depending on the network requirements. In a single firewall architecture, assuming at least three network interfaces, the external network is formed from the ISP to the firewall on the first network interface. The internal network is formed from the second network interface, and the DMZ is formed from the third network interface. Different sets of rules for traffic tightly control which ports and types of traffic are allowed into the DMZ from the Internet. This limits connectivity to specific hosts in the internal network and prevents unrequested connections, either to the Internet or the internal LAN, from the DMZ.

We have used multiple firewalls to create a DMZ. The first firewall is configured to allow traffic destined to the DMZ only. The second or internal firewall only allows traffic from the DMZ to the internal network. This is considered more secure since two devices would need to be compromised before an attacker could access the internal LAN. As a DMZ segments a network, security controls can be varied specifically for each segment. For example, a network intrusion detection and prevention system located in a DMZ containing a Web server could block all traffic except HTTP and HTTPS requests on ports 80 and 443.

Malware Detection and Protection (MDP) Services

Experience: At the NRC, G2SF is moving the enterprise wide malware and antivirus software from Symantec 12 to Symantec 14. This upgrade is easily done from within the Symantec Enterprise Protection Managers. Once the managers are upgraded, we will pilot groups of workstations and servers. Full deployment to the enterprise is accomplished by moving computers into upgrade folders within the tool. G2SF has been managing the current Symantec for six years and has management consoles and email alerts on any type of virus or malware activities. The logs are forwarded to QRadar and Splunk SIEMs to correlate with network activities and baselines.

When an outbreak is detected, the G2SF SOC has many tools at its disposal to limit lateral movement and isolate the offending machines. First, Symantec can begin remediation and isolation efforts. Next, ForeScout CounterACT can either ACL restrict or completely shut down the switch port. The SOC issues trouble tickets from Remedy directly to desk-side support personnel to visit and remediate the workstations. All actions and activities are recorded by the SOC and later reported internally on an Archer system, then ultimately to US-Cert. A next-generation antivirus product that is currently under study claims to utilize Microsoft's image restore facility to remediate infected machines, but that product and capability are not yet in use at the NRC.

Capabilities: G2SF recognizes that agencies go to great lengths to protect sensitive data with firewalls and access security systems. We take a multifaceted approach to malware detection and protection. Proactively, we conduct social engineering assessments. Reactively, we have significant experience scanning for malware. Both approaches are discussed below.

We recognize that hackers exploit security weaknesses on servers to gain access to websites to install malicious code. They then use that website to spread viruses, hijack computers and steal sensitive data. Malware code is not easily detected, yet our staff has significant experience conducting vulnerability assessments to identify the most critical vulnerabilities. G2SF has experience with a variety of tools to conduct daily scans for website malware and automatic weekly scans that look for vulnerabilities. Once malicious code is hidden within the source code, it can be difficult to detect without a line-by-line analysis. If malware is detected, an incident is created, and an Incident Response is triggered. Our experience with incident response is discussed below in Section 2.9. In addition to the tools mentioned above, G2SF staff has experience working with a wide range of vulnerability management tools including:

- Assured Compliance Assessment Solution (ACAS)
- Security Content Automation Protocol (SCAP)
- Tenable Nessus and SecurityCenter Suite
- QualysGuard
- BeyondTrust Retina
- Rapid7 Nexpose
- Trustwave AppDetective
- Imperva Scuba
- HP WebInspect
- Acunetix Scanning Suite
- Burp Suit

However, it has been our observation that most often the weakest link in data defenses is an organization's own people. Today's threats take advantage of basic human behavior to get access to data and systems. Social engineering is a non-technical intrusion that tricks unsuspecting individuals into breaking normal security procedures and giving network access to attackers. Often, this results in malware being placed within the enterprise. A typical approach to exploit an organization's employees is:

- Phishing – Email phishing is one of the most common social engineering methods. Users of critical data are tricked into revealing passwords or clicking on links that contain malware. To

prevent this, G2SF conducts controlled phishing assessments in order to measure employees' IT security awareness. Once the assessment is complete we provide the results and suggestions to the training organization or can conduct training upon request.

Security Event Management Services

Experience: At the NRC, G2SF delivers a full security service which includes Intrusion Management (IM). Using the Protect and Detect portions of the service delivery, the G2SF team takes input from all sources to identify intrusions. Once identified, the intrusions are quickly triaged for scope and impact. Many process flows have been created to guide the team during the information gathering phase. Once identified, the team strives to create indicators of compromise (IOCs) that can quickly be deployed on all IT assets around the enterprise. The who, what, where and how are collected and formulated into after-action reports as well as mandated regulatory reports to DHS's US-Cert. RSA's Archer software is used to gather information and keep a record of all incidents at the NRC. Archer also creates the XML to forward to US-Cert. G2SF's team takes control and responsibility during the event and follows through on all actions until the event is deemed remediated.

Capabilities: G2SF has the capability to control and dynamically adapt intrusion detection configurations and policies or enact response within the appropriate context. We understand this is not the same as the Security Information and Event Monitor (SIEM). Our team understands that the primary facets of IM are:

- Element management (administering the individual detection and response components)
- The processes for determining and executing detection or response tactics (signatures, configurations, policies, etc.)
- The infrastructure for deploying intrusion architecture and protection services (including reporting and alerting)
- The interfaces to other services

G2SF can provide system administration of the individual devices and software in accordance with Service Level Agreements to enable central reporting or export of logs of events and alerts (either to the provider or the SIEM service). This may include protocol, data format, and administrative management of the device. Intrusion Management infrastructure includes the appropriate network, system, and software configurations to support the transmission, access, and organization of data elements to support the following:

- Central Reporting of events and alerts (either to the provider or the SIEM service)
- SIEM Integration
- Administrator Notification for issues with service elements
- Customization of Policy (automatic or manual) and other configurations
- Mapping to Cloud-layer Tenancy (both in deployment as well as management and reporting)
- Cloud Sourcing Information to reduce false positives and improve coverage
- Remote Storage or Transmission of integrity information, to prevent local evasion

G2SF understands that to protect the enterprise, one should expect and anticipate the infrastructure's connectivity (the data systems communicating over the network) will be compromised which will impact alerting, reporting and access to protection systems. The inability to control devices remotely during an attack, or in the event of outage may be significant. G2SF staff considers this when assessing the infrastructure's ability to support IM and when developing strategies and solutions to mitigate risk.

Security Incident Management

Experience: At the NRC, G2SF's security incident handling service is closely tied to the Intrusion Management Service. Intrusion management is a subset of security incident handling. The process is almost identical, differing only in attack vector or initial reporting mechanism. For example, a classified information spill in unclassified email may be reported by the end user community and an intrusion event may be alerted by the G2SF operated SIEM. After such a security incident, action reports and process improvement steps are conducted to improve the security service for the NRC.

Capabilities: G2SF understands a Computer Security Incident Response Team (CSIRT) is a service organization responsible for receiving, reviewing, and responding to computer security incident reports and activity. Even the best information security infrastructure cannot guarantee that intrusions or other malicious acts will never happen. When computer security incidents do occur, G2SF responds effectively and efficiently.

The speed with which an agency can recognize, analyze and respond to an incident will limit damage and lower the cost of recovery. A G2SF incident response team is available to be deployed on site to contain a computer security incident and recover from it quickly. CSIRTs also have familiarity with the compromised systems and are able to coordinate the recovery, mitigation and response strategies almost immediately.

Additionally, their relationships with other CSIRTs and security organizations facilitate the sharing of response strategies and early alerts to potential problems. Proactively, CSIRTs work with other areas of the organization to ensure new systems are developed and deployed with "security in mind" and in conformance with any site security policies. They can help identify vulnerable areas of the organization and, in some cases, perform vulnerability assessments and incident detection.

Audit and Accountability Services

Experience: At the NRC, G2SF has designed the enterprise deployment of Splunk to fulfill the audit and accountability function. By utilizing centralized log aggregation, ISSOs, system administrators and security personnel develop queries and reports on pertinent audit and accountability measures. Splunk meets or exceeds requirements laid out in NIST's 800-53 rev.4 Access Controls (AC) and Audit and Accountability (AU) families for security categorization High systems. The automated reports allow ISSOs and system administrators to perform their required log reviews in a much more effective and automated manner. Higher level patterns and trends can be seen by the reports and dashboards, ultimately giving a better representation of security posture for the whole enterprise instead of just one system or user.

Capabilities: Multiple compliance requirements slow down agencies' abilites to focus on their mission. Most agencies are faced with significant compliance requirements. G2SF staff understands this and works with agency security personnel to optimize the audit process by sequencing the work, centrally managing risk, and leveraging testing efficiencies. We do this by mapping controls across multiple compliance areas, allowing for more structured and coordinated audit processes that improve the overall efficiency of testing and reporting activities. The results are:

- More efficient audits that can be run concurrently based on control mappings
- Audit activities span multiple regulatory standards and domains
- Better visibility of end-to-end controls
- Reduction of effort and associated costs based on the identification of common controls across multiple compliance areas

Data Destruction Services

Experience: At the NRC, G2SF operates the product, Jetico Central Manager with BCWipe. This tool is used to give Military overwrite capabilities for file removal activities. It enables a single person (Administrator) from a central administration computer to control all functions, including the initial installation of the Administration Database on a Server and BCWipe client software, on any number of remote workstations. Once malware, virus or data spill files are identified, the Jetico Central Manager wipes files enterprise-wide and keeps logs of progress and success. It also allows administrators to run scheduled tasks to wipe data on remote workstations across the enterprise, if necessary. In the case of simple virus or malware files, Symantec Endpoint Protection Manager is also used. If a file or system cannot be successfully cleaned, then system re-imaging is performed using Microsoft SCCM. In some cases, EnCase is also used to perform forensics activities on systems.

Capabilities: As part of our overall SOC service offering, we have the experience and staff to identify and define the specific criteria for file wiping on mobile, local and remote devices and workstations. Once the criteria are defined, in accordance with federal and agency policies, G2SF staff can assist in developing the policies and procedures for wiping files. Our experience with multiple technologies enables us to ensure that files are wiped quickly and efficiently, reducing exposure and risk. We can assist with the development of "rules of behavior" for Bring Your Own Device (BYOD) solutions, utilizing our experience in support of this area at the NRC. This includes the process of developing policies outlining the causes for the agency to remotely wipe personal devices. Rules of behavior are signed off on by each individual user prior to allowing the device to connect to the network.

Risk Management Framework and Certification and Accreditation (C&A) Services

Experience: G2SF has experience with both DoD Instruction 8510.01 RMF at the US Marine Corps, Quantico, VA and NIST Special Publication 800-37 Revision 1 RMF at the NRC. As part of G2SF's current ITSM Operations and Maintenance contract in support of the USMC, G2SF was tasked with providing security requirements identification, analysis, allocation, and tracking support utilizing the Defense Information Assurance Certification and Accreditation Process (DIACAP). This included assisting the Government in retaining the Authority to Operate (ATO) throughout USMC ITSM Suite upgrades and capability improvements, as well as developing and editing accreditation packages for the training, pre-production, and production environments. In support of these requirements, G2SF System Engineers and IA specialists created and maintained a Plan of Actions and Milestones (POAMs) for five (5) Remedy environments and remediated or mitigated findings discovered during Assured Compliance Assessment Solution (ACAS) and Security Content Automation Protocol (SCAP) scans. G2SF ensures adherence to all DOD and USMC standards and regulations while providing the documentation and information needed to obtain, maintain, and re-certify the ITSM systems ATO. G2SF assisted in answering data calls as packages progressed through the DIACAP and Risk Management Framework (RMF) processes during the Remedy 7.5 to 8.1 system upgrade.

At the NRC, G2SF operates an Information Assurance team operating under NIST 800-53 rev.4 guidance. This team performs all aspects of Risk Management under NIST 800-37 rev.1. The G2SF team provides the security service for the largest FISMA system at the NRC. The system represents over 98% of total IT assets. This FISMA system is comprised of seven subsystems, including:

- Core
- Common Computing
- ICAM
- Workstations
- Printers and Peripherals
- Mobility
- Telecom

Core is made up of security devices and networking. G2SF generated and maintains all of the base documentation for the SSP and participates in all C&A and ST&E activities. Due to separation of duties, G2SF supports, supplies and manages all aspects of the Certification and Accreditation process, then an independent IV&V contractor validates documentation and findings and presents the results to the DAAs.

Capabilities: The transition from DIACAP to the Department of Defense (DoD) Risk Management Framework enables agencies to effectively manage the lifecycle cyber security risk to IT and make better informed, risk-based decisions.

G2SF staff has decades of policy experience and knowledge and can help address the challenges to successfully transition ACE IT programs, as needed. Our Risk Management Framework (RMF) approach to cybersecurity builds on the framework's 6 steps (Categorize, Select, Implement, Assess, Authorize, Monitor) by capitalizing on our extensive experience delivering RMF services at the NRC and USMC.

We understand that the transition from DIACAP to the DoD Risk Management Framework presents multiple challenges for organizations, including:

- Changing traditional certification and accreditation (C&A) processes
- Implementing new cybersecurity controls
- Adopting new terminology for cybersecurity roles and processes
- Shifting roles and responsibilities

To address these challenges, we assist clients by:

- Performing a gap analysis of existing processes and technologies
- Identifying the scope of work required to fully implement DoD RMF requirements
- Leveraging current documentation and procedures, wherever possible
- Developing and implementing risk-focused tools and procedures
- Delivering a compliant cybersecurity program focused on risk-based decision making

G2SF capitalizes on our experience in Continuous Diagnostics and Mitigation (CDM), network and systems assessments, and cybersecurity integration with the System Development Life Cycle (SDLC) to implement a comprehensive cybersecurity program that provides complete cyber risk management, not just C&A packages. Furthermore, we integrate the Project Management Institute (PMI) and ITIL and ISO 9001:2015 methodologies on all DoD RMF efforts to ensure consistency, repeatability, quality, and efficiency.

We can utilize our expertise to seamlessly migrate any ACE IT programs or projects. This includes:

- Tailoring the RMF to ACE IT while aligning supporting functions to realize framework efficiencies
- Integrating the ACE IT System Development Life Cycle (SDLC) and acquisition system activities to ensure a cost-effective transition from the beginning
- Providing continuous monitoring for near real-time decisions
- Leveraging similarities in control implementation to consolidate systems into logical boundaries
- Producing fewer C&A packages and reducing the amount of resources needed to complete the overall process

The G2SF DoD Risk Management Framework services approach to cyber security allows organizations to:

- Gauge potential impact of risk-based decision making on the mission

- Reduce time spent obtaining DoD and other federal agency authorizations with reciprocal acceptance
- Increase the likelihood of executing future projects on time and on budget by building security into systems proactively
- Enhance efficiency through information assurance control inheritance, consistency, and reuse

Accreditation Records Management

Experience: At the NRC, the G2SF security team has acquired considerable experience executing, managing and validating security/IA requirements in all aspects of Federal, Military and Commercial security programs. G2SF NRC security personnel have worked with DIACAP, DoD RMF, National Information Assurance Certification and Accreditation (NIACAP), Federal Information Security Management Act (FISMA), Director of Central Intelligence Directives (DCID) 6/3 (and its replacement Intelligence Community Directive (ICD) 503). They are actively addressing the changes instituted in the recently released National Institute of Standards and Technology (NIST) 800-53 revision 4. The G2SF security team has taken a practical, best of breed approach to working on NIST 800-53 revision 4 requirements and has integrated the standards into new and emerging NRC projects to address the controls necessary to fully secure the technology. These are documented and captured as working drafts. Updates are made as frequently as necessary to reflect changes to the systems as upgrades or addressing previously identified issues. Typically, at the end of every quarter, final updates are made to the documents and final versions are uploaded to the Agencywide Documents Access and Management System (ADAMS), the official record keeping system of the NRC. G2SF has routinely evaluated the existing controls for NRC systems that allow for a cycle of continual improvement before controls become findings or vulnerabilities. G2SF has responsibility for coordinating with commercial providers, including the United States Computer Emergency Readiness Team (USCERT), as well as multiple Operations and Maintenance (O&M) contractors to provide comprehensive security services for the NRC. The G2SF team has also used Telos Xacta to maintain accreditation records in support of the NRC.

Capabilities: G2SF is familiar with the eMASS Government off-the-shelf (GOTS) solution that is used for a variety of different services, including accreditation documentation management. We have supported its use at the USMC for the generation of Risk Management Framework (RMF) for Department of Defense (DoD) Information Technology (IT) and DoD Information Assurance Certification and Accreditation Process (DIACAP) Package Reports. We have provided the documentation in accordance with regulations and policies to support its use in the management of cybersecurity compliance activities and the maintenance of an enterprise baseline for security controls. The documentation is then stored in the eMASS repository and updated with industry standards, as necessary. G2SF has experience using the system to allow product teams, testers and security control assessors to collaborate and share documentation with Integrated Project Teams in multiple global locations.

Security Control Testing

Experience: At the NRC, G2SF utilizes NIST Special Publication 800-53, Recommended Security Controls for Federal Information Systems and Organizations and 800-53A, Guide for Assessing the Security Controls in Federal Information Systems and Organizations. Each publication provides guidance for implementing specific steps in the RMF. Special Publication 800-53 covers Step 2, security control selection (i.e., determining what security controls are needed to manage risks to organizational operations and assets, individuals, other organizations and the Nation). Special Publication 800- 53A covers Step 4, security control assessment, and Step 6, continuous monitoring.

In accordance with NIST guidelines and NRC policy, G2SF operates the enterprise-wide vulnerability and compliance scanner. In previous years, nCircle and DISA Gold disk were used to perform security controls testing but have since been retired. By operating the always-on continuous monitoring system

(Tenable), G2SF personnel, ISSOs, and IV&V auditors have access and visibility to real-time data on the security posture of any asset on the enterprise-wide network. If an asset has not yet been connected to a production or testing area, then mobile Nessus scanners are used, and the data is later uploaded into the centralized Tenable Security Center instance. This ensures that DAAs, ISSOs and system administrators have continual access to current data on the security posture of assets and systems within the NRC enterprise network.

The Tenable system is used for three primary types of scans:

- Non-authenticated vulnerability scans
- Authenticated vulnerability scans
- Authenticated compliance scans

The G2SF team and the NRC have created a policy to install DISA STIG SCAP data twice a year. At the same time, the Tenable system updates plugins every day. This provides the best security vulnerability scanning possible, but also allows system owners time to meet STIG compliance scanning without constantly changing the metrics by which systems are held accountable.

Based on assessment and testing/scanning results, G2SF currently provides the following support for the NRC and the USMC:

- Identifies weaknesses in patching and configuration management
- Develops configuration and patch management plans and procedures
- Prioritizes security findings for efficient resolution; Critical, High, Medium and Low
- Implements remediation actions based on prioritizations
- Tests for compliance
- Identifies security weaknesses using a blue team approach

Capabilities: G2SF understands that security control assessments are not about checklists, simple pass-fail results, or generating paperwork to pass inspections or audits. Security controls assessments are the principal vehicle used to verify that IT systems are meeting the agency's stated security goals and objectives. Reactive security measures are insufficient to prevent a security breach or minimize its impact. G2SF has many years of experiencing implementing proactive approaches to vulnerability management, building on our experience designing complete cybersecurity programs, including ongoing management to ensure consistent, complete and compliant security processes. In accordance with Federal and DoD regulations and polices we can assist with:

- Recognizing, managing and reducing cyber-related threats more efficiently
- Determining where additional internal oversight may benefit project teams
- Conducting thorough technical assessments of hosts, databases, and applications to identify deficiencies
- Developing configuration management and patch management plans and procedures
- Identifying the aggregate level of security

G2SF staff has experience with new risk management methods designed to combat new challenges, including the Department of Homeland Security's Continuous Diagnostics and Mitigation (CDM) and the NIST Information Security Continuous Monitoring (ISCM). Specifically, G2SF has experience with delivering and supporting:

- **Baseline Capabilities Assessment –** to gain insight into current maturity levels and ISCM/CDM capabilities based on current people, processes, and technologies

- **ISCM Strategy/Policy –** to provide strategic and tactical logistical steps for each capability to migrate from current maturity levels to an environment of near real-time risk management, as required by OMB M-14-03
- **Risk Scoring –** to enable planning and mitigation decisions by identifying a comprehensive risk picture
- **Architecture Planning –** for ISCM/CDM maturity growth with an architecture that creates and integrates ISCM/CDM subsystems to support scalable modeling and planning
- **Requirements Engineering –** to identify technical requirements for business and mission objectives that impact the development, implementation, and integration of an ISCM/CDM solution
- **Data Integration and Implementation –** to deploy and maintain a holistic, efficient monitoring solution by integrating disparate tools and sensors, data extraction, parsing, and normalization to develop an accurate risk view
- **Data Analytics and Visualization –** to correlate integrated and normalized risk-related data to produce actionable information
- **Ongoing Authorization –** to migrate legacy authorization processes to a more efficient, accurate, and near real-time model that significantly reduces assessment and compliance costs
- **Governance –** to develop foundational elements including policy, organizational structure, engineering lifecycle management, outreach and training

Penetration Testing

Experience: At the NRC, G2SF participates and coordinates WhiteHat (full knowledge) level penetration testing. Tools that G2SF uses on the WhiteHat side of penetration testing include, but are not limited to, WebInspect, Qualys, Tenable, Nessus, and Nmap.

Capabilities: Team G2SF's penetration tests, whether internal or external, white-box or black-box, are designed to emulate the threat landscape our customers face. We have developed an adaptive penetration testing methodology, leveraging industry best practices, that focuses on real threat sources specific to a target environment to develop relevant attack vectors. This methodology enables us to reduce the time and cost required, while performing comprehensive penetration tests that meet government agency requirements. The tests are consistent, repeatable, and measurable within tightly-defined testing periods to provide clients with valuable insight into the real-world risks of system vulnerabilities and mission impact of network intrusions.

Team G2SF's approach thoroughly analyzes customer systems and identifies vulnerabilities and potential attack vectors. We attempt to leverage publicly available exploitation techniques if available or build custom exploits to penetrate the infrastructure if needed. Penetration testing can range from breaching single hosts to gaining deep access into the network, based on customer requirements. Penetration testing services include:

- Red-team and Blue-team assessments
- External network penetration tests to identify and target externally exposed attack surfaces and simulate outside attackers
- Internal network penetration tests to assess a system's resistance to attacks by insider threats
- The G2SF testing methodology follows a standard three-phase process:

Enumeration

- Network mapping and host discovery
- Service identification, vulnerability scanning, and web application discovery
- Identification of critical systems and network protections

Exploitation

- Research exploits and attacks based on enumerated information
- Active exploitation of vulnerable systems and applications
- Manual testing tailored to the deployment and business purpose of the target

Escalation

- Escalate privileges and compromise credentials
- Leverage compromised systems to gain new access further into the network
- Attempt to access business critical systems or information to demonstrate impact

Team G2SF brings significant experience supporting government agencies with comprehensive technical security services. G2SF ensures all tests and assessments are effectively executed within an agreed upon timeframe by prioritizing the testing of critical devices and components. This ensures efficient penetration tests that maximize resources. We provide our customers with valuable and actionable results including discovered vulnerabilities, potential attack paths, mission impact of breaches, and remediation steps to reduce exposure. Our staff have a number of industry certifications, including GPEN, GCIH, GWAPT, CREST CCT, MCSE, RHCT, OSCP, OSCE, NSA IAM/IEM, CEH, PMP, and CISSP.