EFCOG Cybersecurity Working Group FY 2022 Annual Work Plan (October 1, 2021 – September 30, 2022)

Purpose

This document contains the Energy Facility Contractors Group (EFCOG) Cybersecurity Working Group (CSWG) FY 2022 Annual Work Plan (AWP). The approved AWP provides authorization for EFCOG members within the various subgroups to work on activities identified in the AWP.

Cybersecurity Working Group Mission and Objectives:

The EFCOG CSWG is chartered to assist member companies to attain and maintain excellence in all aspects of Cybersecurity operations and management of DOE facilities through the consistent exchange of information, best practices, and corresponding improvement activities. The CSWG will achieve this by:

- Leveraging the expertise and experience of DOE Contractors to address challenges and achieve improvements in cybersecurity;
- Advocating for strong, effective implementation of Integrated Cybersecurity Management across departmental activities;
- Developing, and promoting best management and operating practices;
- Improving the effectiveness of boundary authorization packages for achieving and maintaining the Authority to Operate (ATO) and achievement of Cybersecurity readiness processes across contracts by working together, exchanging information, and sharing best practices and lessons learned;
- Improving the effectiveness of risk management and cyber resilience, and associated processes by developing tools, practices, guidance, and recommendations for compliance and directive changes – where appropriate and as supported by Contractor and DOE line management;
- Providing real-time support for cyber related emergent issues in the form of ideas, tools, resources, etc.;
- Interfacing with various intelligence associated organizations and industry providers to promote cooperation, information exchange, and as appropriate, minimization of duplication of effort;
- Interfacing with key DOE managers (both headquarters and field) on varying concepts, practices, and concerns associated with Cybersecurity needs and processes to enable better understanding of customer needs and concerns;
- Interfacing with other external organizations on varying concepts, practices, and concerns associated with Cybersecurity

processes and risk management;
- Promoting transparent communications across group members and DOE;
- Facilitating the exchange of operating experiences and information on Cybersecurity programs and their effectiveness, and designing studies and developing position and technical papers to inform DOE where appropriate;
- Providing DOE and member companies with access to a network of subject matter experts;
- Identifying opportunities to save and/or avoid costs in the implementation of Cybersecurity and regulatory programs while assisting member companies to implement effective Cybersecurity and regulatory programs through peer reviews and consultations; and
- Arranging training and awareness workshops and collaborative workshops to enhance the competency of Cybersecurity professionals.

The working group is focused around the following key areas of Cybersecurity: Industrial Control Systems/Distributed Control Systems/SCADA; IoT & Smart Technologies; Risk Management & Governance; Addressing Remote Work Challenges; Technology and Tools; and Cloud Security.

CSWG FY2021 Accomplishments

- Established multiple cybersecurity best practices associated with remote work.
- Arranged and scheduled key speakers for a CSWG Workshop to be held in October 2021 during Cybersecurity Awareness Month.
- Reviewed abstracts for key topics for CSWG Workshop.
- Updated the secure platform in a FedRAMP tenant of Azure Government for conducting the collaborative workshop and online discussion forum.
- Began establishing subgroups for CSWG.
- Created Charter for a Cybersecurity Center of Excellence.
- Initiated planning for integrating Cybersecurity in the Safety and Quality Assurance Framework.
- Established best practice documentation for key areas.
- Facilitated Cybersecurity awareness through distribution of current threats and current events.
- Assisted in planning activities to support compliance with Binding Operational Directives.
- Completed best practice for Cyber resilience in a remote environment

CSWG Focus Areas for FY22

- Finalize initial subgroups for key topic areas
- Conduct the CSWG Workshop for October 2022 in alignment with Cybersecurity Awareness Month

- Build the framework and personnel to support the Cybersecurity Center of Excellence
- Begin building the framework for integrating Cybersecurity into the Safety and Quality Assurance process
- Establish key cybersecurity metrics that site leadership should be aware of on a consistent basis
- Participate in planning and execution of Ransomware preparation and response exercises
- Facilitate additional participation across DOE and the EFCOG contractor community
- Continue collaboration in the CSWG discussion forum to facilitate key topic discussions, generate best practices, and share information
- Turn the collaboration from the CSWG Workshop into best practices and additional action items to further the cybersecurity capabilities across sites
- Conduct lessons learned from CSWG Workshop to use for improving the platform and effectiveness for the October 2022 event
- Plan the October 2022 event with speakers and topic areas
- Prepare an EFCOG CSWG session for the DOE Cybersecurity Conference
- Create and make available vendor neutral white papers on key topic areas
- Create and make available best practice guides for key topics such as:
    - NIST 800-53 rev 4 to rev 5 security plan conversions
    - NIST 800-53 rev 4, rev 5 and Cybersecurity Framework (CSF) mapping guide
    - NIST 800-53 rev 5 with NIST 800-82 overlay security plan template
    - Cyber resilience practices - top 10+
    - Cloud Security practices – top 10+
    - Understanding, categorizing, and protecting High Value Assets
    - Industrial Controls Security top 10+
    - Smart technologies security top 10+
    - Tool considerations/comparisons for Identify, Protect, Detect, Respond, and Recover capabilities

Working Group Activities

The CSWG leadership will conduct group conference calls as necessary to discuss activities and progress. These calls will be scheduled to last one hour and typically involve 5-15 people. If available, the DOE and EFCOG liaisons will be invited. Total time invested is approximately 10 hours/month.

Subgroups may additionally have the same type of meetings as described above. Participation may be 10-25 people. Total time invested is approximately 8-15 hours/month.

An overall CSWG annual meeting will be held to bring Contractor, Federal, and Industry members together. This may occur in a face to face forum, providing health and safety concerns are not an issue due to pandemic concerns. If face to face is of concern or if an

online forum is deemed more effective, an online forum will be created to facilitate a virtual set of meetings to allow for breakout sessions where deliverables are reviewed, edited, deliberated on, and emerging issues identified. Attendance will potentially involve 100-200 personnel and total costs will not exceed the $100K threshold requiring additional approvals. In person meetings will be held at DOE sites to reduce overall costs and to facilitate other related business activities.

EFCOG Cybersecurity Working Group Planned Activities for FY 2022
(October 1, 2021 – September 30, 2022)

Activity(s)	Benefit(s)	Deliverable/Key Milestone(s)
1.0 Cybersecurity Awareness & Collaboration		
1.1 Increase Cybersecurity Awareness across EFCOG	Increasing Cybersecurity awareness across the contracting organizations will result in overall improved understanding of cybersecurity risks and challenges.	1.1.1 Non-sensitive cybersecurity awareness materials for distribution/publication to EFCOG team members 1.1.2 Distribute, and/or publish materials, based on EFCOG member preference 1.1.3 Create high level Cybersecurity awareness training course to provide to EFCOG members who wish to attend 1.1.4 Offer course in an online forum, and record for playback for anyone who was unable to attend who may want to view later 1.1.5 Provide an online Cyber Awareness Workshop in the month of October as part of Cybersecurity Awareness Month
1.2 Enhance Cybersecurity collaboration capabilities	Increased collaboration will strengthen cybersecurity capabilities and advance the risk management program across DOE sites.	1.2.1 Create collaboration forum for sharing moderate level data in an approved location with multi-factor authentication and moderate security controls
1.3 Collaborate on key issues such as ransomware preparation and response across sites	Increase awareness in overall processes and help to establish best practices around the key topic of ransomware preparation and response	1.3.1 Identify site to lead 1.3.2 Identify key participants 1.3.3 Participate in tabletop event 1.3.4 Identify lessons learned

Activity(s)	Benefit(s)	Deliverable/Key Milestone(s)
1.4 Establish Cybersecurity Center of Excellence	Access to SME support for key cybersecurity issues across all sites and ability to leverage resources effectively.	1.4.1 Obtain charter approval. 1.4.2 Identify key Cybersecurity areas for structure 1.4.3 Establish an online forum for communications 1.4.4 Identify key resources for each area 1.4.5 Identify funding source
1.5 Establish framework to integrate cybersecurity into safety and quality	Leverage a proven methodology to integrate cybersecurity into operational processes	1.5.1 Define requirements 1.5.2 Establish framework
1.6 Identify issues for focus for next FY	Focus sub-group for next FY	1.6.1 Update Annual Work Plan to reflect focus issues
2.0 Cybersecurity Best Practices		
2.1 Develop best practice for creating authorization packages (C&A packages)	Best practices for C&A packages will provide a roadmap for compliance, promote standardization, and reduce time in package creation.	2.1.1 C&A package creation checklist 2.1.2 C&A Package templates
2.2 Develop best practice for ensuring compliance in handling government data on corporate information systems	Best practice documentation for handling DOE data on corporate information systems will help member companies understand and reduce risks, as well as improve information security of DOE information.	2.2.1 Develop “Handling and protecting government data on corporate information systems” best practice document
2.3 Create a master list of cybersecurity best practice documents that are needed to facilitate an improved cybersecurity posture	Best practice documentation will improve productivity, support standardization, and facilitate an overall improved cybersecurity posture.	2.3.1 Work with DOE to determine if a Cybersecurity Best Practice Handbook will be beneficial 2.3.2 Work with team members and parallel teams with similar concerns, such as the Security Working Group, to collaborate on documents needed that will support overall improvements
2.4 Identify issues for focus for next FY	Focus sub-group for next FY	2.4.1 Update Annual Work Plan to reflect focus issues

Activity(s)	Benefit(s)	Deliverable/Key Milestone(s)
3.0 ICS Security		
3.1 Facilitate participation in the ICS Sub-Group and work closely with established DOE ICS Working Group to leverage information and collaboration activities	Collaboration with existing subject area groups will reduce duplication efforts and increase knowledge sharing capabilities.	3.1.1 Identify ICS subject matter experts across the member sites to collaborate on best practices and common issues 3.1.2 Facilitate collaboration activities with the DOE ICS Working Group
3.2 Identify common issues across ICS and subject matter experts who can provide input to common solutions	Common issue identification will help team to focus on the issues with the greatest impact.	3.2.1 Common issue list with SME list
3.3 Identify Industrial Controls Security Top 10+	Identification of the top 10+Industrial Controls System Security top 10+ issues currently or that will affect the EFCOG members soon allows us to prepare for them.	3.3.1 Industrial Controls Security Top 10+ list.
3.4 Identify issues for focus for next FY	Focus sub-group for next FY	3.4.1 Update Annual Work Plan to reflect focus issues
4.0 Smart Technology/ IoT Security		
4.1 Establish sub working group to initiate working group activities	This action is to get the sub-group started.	4.1.1 Establish sub-group membership 4.1.2 Establish sub-group leadership
4.2 Gather data for how Smart Technology/IoT security concerns are applicable at DOE projects	This will help to define the issues as they relate to DOE.	4.2.1 Unofficial data call determining what is being seen across the sites and projects
4.3 Identify Smart technologies security top 10+	Identification of the top 10+ Smart Technologies in use or that will affect the EFCOG members soon allows us to prepare for them.	4.3.1 Smart Technology security top 10+ list.
4.4 Identify issues for focus for next FY	Focus sub-group for next FY	4.4.1 Update Annual Work Plan to reflect focus issues

Activity(s)	Benefit(s)	Deliverable/Key Milestone(s)
5.0 Risk Management and Governance		
5.1 Establish sub working group to initiate working group activities	This action is to get the sub-group started.	5.1.1 Establish sub-group membership Establish sub-group leadership
5.2 Understanding, categorizing, and protecting High Value Assets	There is an ongoing debate regarding what a high value asset is and the ramifications of being a high value asset. This will help define it for the EFCOG members in a consider and consistent manner.	5.2.1 EFCOG High Value Assess Handbook
5.3 Identify issues for focus for next FY	Focus sub-group for next FY	5.3.1 Update Annual Work Plan to reflect focus issues
6.0 Technologies and Tools		
6.1 Establish sub working group to initiate working group activities	This action is to get the sub-group started.	6.1.1 Establish sub-group membership 6.1.2 Establish sub-group leadership
6.2 Tool considerations/comparisons for Identify, Protect, Detect, Respond, and Recover capabilities	Utilizes the EFCOG to help create a better comparison than any single member can achieve.	6.2.1 Tool consideration/comparison whitepapers and potentially volume discounts.
6.3 Identify technology and tool areas to focus on for next FY	Focus sub-group for next FY	6.3.1 Update Annual Work Plan to reflect focus areas
7.0 Cloud Security		
7.1 Establish sub working group to initiate working group activities	This action is to get the sub-group started.	7.1.1 Establish sub-group membership 7.1.2 Establish sub-group leadership
7.2 Identify Cloud Security Top 10+ issues	Identification of the top 10+ Cloud Security Top 10_ issues for 2021 or that will affect the EFCOG members soon allows us to prepare for them.	7.2.1 Cloud Security Top 10+ list
7.3 Identify issues for focus for next FY	Focus sub-group for next FY	7.3.1 Update Annual Work Plan to reflect focus areas

Activity(s)	Benefit(s)	Deliverable/Key Milestone(s)
8.0 Next FY Plan		
8.1 Identify issues for focus for next FY	Focus sub-group for next FY	8.1.1 Update Annual Work Plan to reflect focus issues