Task Force on Developing PSCC S Subcommittee Activity Roadmap

| Category | Topic | Description | Recommended  Activity | Survey Priority  (H/M/L) |
| --- | --- | --- | --- | --- |
| **Data Transport and Application Protocol**  **(HIGH 24)** | STTP |  |  | LOW |
| C37.118.2 | IEEE Synchrophasor Protocol |  | MEDIUM |
| **HTTPS** | **Secure HTTP** | **Standard for applying https and TLS to devices used in electric power system operations (including DER)** | **HIGH** |
| SFTP | Secure FTP |  | LOW |
| SSH | Secure Shell (SSH) |  | MED |
|  |  |  |  |
| **Authentication and Transport Encryption**  **(HIGH 22)** | **TLS** | **Transport Layer Security (SSL)** | **Included HTTPS** | **HIGH** |
| IPSEC | Interoperability of IPSEC for power systems |  | MEDIUM |
| RADIUS | Remote Authentication Dial-In User Service |  | MEDIUM |
| GDOI | Group Domain of Interpretation |  | LOW |
| **IEC 62351-6** | **Security for IEC 61850 including GOOSE and Sampled Value messaging for Ethernet and IP Multicast** | 1. Recommended practice on implementing security for IEC 61850 including GOOSE and Sampled Value messaging for Ethernet and IP Multicast 2. Evaluation of other IEC 62351 parts for inclusion in IEEE S0 activities. | **HIGH** |
| TACACS | Cisco version of RADIUS (simplistically) |  | LOW |
| SSH | Secure Shell (SSH) |  | MEDIUM |
| LDAP | Lightweight Directory Access Protocol |  | MEDIUM |
|  |  |  |  |
|  |  |  |  |
| **Intrusion / Resiliency / Response**  **(HIGH 20)** | **IDS** | **Intrusion Detection Systems** | **Recommended practice for applying IDS/IPS (Malicious code detection)** | **HIGH** |
| **IPS** | **Intrusion Prevention Systems** | **HIGH** |
| Graceful Degradation of Systems | How to respond in order to maintain system availability and integrity |  | MEDIUM |
| **Cyber resiliency** | **Common mode vulnerabilities** |  | **HIGH** |
| Power System Physics Monitoring | Using the physics/state of the power system to evaluate the occurrence of a cyber event |  | MEDIUM |
| Forensics |  |  | LOW |
| Penetration Testing | How, when and why to perform Pen Testing on power system equipment and its impact |  | LOW |
| Threats, Threat Actors and Impacts | Report or Guide to help utilities understand |  | LOW |
| Incident Response |  |  | LOW |
| Certificate Management  (MEDIUM 17) | **X.509** | **Certificate format** |  | **HIGH** |
| EST | Enrollment over Secure Transport |  | LOW |
| SCEP | Simple Certificate Enrollment Protocol |  | LOW |
| OCSP |  |  | LOW |
| DKMP | DNP Key Management Protocol |  | MED |
| Design / Architecture  (MEDIUM 17) | **Security Architecture Design** |  |  | **HIGH** |
| General | Security standards |  | MEDIUM |
| Patch Management |  |  | MEDIUM |
| Data Diodes |  |  | LOW |
| SDN | Software Defined Networking |  | LOW |
| SaaS | Software as a Service |  | LOW |
| IEC 62351-8 | Role Based Access Control (RBAC) |  | MEDIUM |
| Logging & Monitoring  (LOW 14) | **Syslog** | **Application profiles for using Syslog for power system monitoring of security functions** |  | **HIGH** |
| SNMP | MIBs for power systems |  | MED |
| General |  |  | LOW |
| Use of Wireless in substation or at the edge in operational systems  (LOW 14) | **802.11** | **Wireless IP Networking** |  | **HIGH** |
| Bluetooth |  |  | LOW |
| Zigbee |  |  | LOW |
| WiMax |  |  | LOW |
| Cellular/5G |  |  | MEDIUM |
| Time Sync Protocols  (LOW 13) | **PTP** | **Precision Time Protocol** |  | **HIGH** |
| IRIG-B | Serial Time synchronization |  | LOW |
| NTP | Network Time Protocol |  | MED |
| SNTP | Simple Network Time Prot. |  | LOW |
| GPS/GNNS | GPS for time synch |  | MED |