Section 34 – IT Infrastructure Hardware and Third-Party System Integration

I. Introduction – This section serves to provide information and standards pertaining to the hardware installation and/or upgrade of HRSD's Information Technology assets, to include new construction, renovation, and third-party integration within HRSD's control network. The objective of this section is to ensure consistency with HRSD's internal policy related to IT infrastructure hardware and to conform to Building Industry Consulting Service International (BICSI) standards as closely as practicable. See attachments A and B for HRSD's technical guidelines related to these topics.

II. General – The objectives are to standardize HRSD’s server and network infrastructure designs as well as HRSD’s processes to accommodate the integration of third-party systems within the control network environment to:

   A. Maximize functionality and performance

   B. Minimize time-to-resolution during troubleshooting efforts

   C. Facilitate the installation or upgrade process by clearly defining expectations so that re-work is minimized

   D. Enhance overall system capability and usefulness

   E. To provide enhanced monitoring and reporting for more streamlined workflows.

III. OT Cybersecurity Requirements – This section establishes requirements pertaining to the cybersecurity of Operational Technology (OT) systems and networks integrated within HRSD environments, including new construction, renovation, and third-party system implementations. The objective of this section is to ensure that OT systems are designed, delivered, and maintained in a secure manner consistent with HRSD’s cybersecurity program and associated standards.

A. All Operational Technology (OT) systems, industrial networks, and associated components shall comply with the HRSD OT Cybersecurity Standards
B. Compliance shall be demonstrated prior to system acceptance and production deployment, including delivery and validation of required turnover artifacts
C. Systems shall be delivered in a secure-by-default state and shall not contain known high or critical vulnerabilities with available patches unless formally approved through the exception process
D. All system changes shall be performed in accordance with the approved Change Management process
E. The OT Cybersecurity Standards shall serve as the authoritative source for OT cybersecurity requirements; IT Infrastructure Hardware Guidelines and Third-Party Control Network Integration Guidelines remain applicable for infrastructure and connectivity, but do not replace OT cybersecurity requirements

IV. Attachments:

A. IT Infrastructure Hardware Guidelines
B. Third-Party Control Network Integration Guidelines
C. Operational Technology (OT) Cybersecurity Standards
D. Operational Technology (OT) Cybersecurity Standards Supporting Guidance
E. Physical Security Infrastructure Standards

End of Section