The Edison Electric Institute (EEI) submits these comments in response to the Department of Energy request for a three-year extension, with changes, to Form OE-417 Electric Emergency Incident and Disturbance Report, OMB Control Number 1901-0288, as required under the Paperwork Reduction Act of 1995. Form OE-417 collects information for DOE to monitor electric emergency incidents and disturbances in the United States. The information collected allows DOE to conduct post-incident reviews examining significant interruptions of electric power or threats to the national electric system.

DOE uses Form OE–417 to monitor electric emergency incidents and disturbances and to investigate significant interruptions of electric power or threats to the electric system reliability. DOE proposes a number of changes most notably to align the reporting requirements with the recently approved North American Electric Reliability Corporation (NERC) CIP–008–6 Reliability Standard, which established new definitions for a Cyber Security Incident and Reportable Cyber Security Incident. Reliability Standard CIP–008–6 also expanded its reporting requirements, including expanding the applicable systems to report on and adding new reporting requirements for attempted compromises of high and medium impact bulk electric system (BES) cyber systems and their associated electronic access control or monitoring systems. DOE states that the continued alignment between Form OE–417 and NERC reporting requirements helps minimize confusion among industry stakeholders about where and how to file reports and enable industry stakeholders to train personnel to report using a single form. By incorporating the requirements established by Reliability Standard CIP–008–6 in Form OE–417, entities may only be required to submit Form OE–417. This change is intended to reduce the overall reporting burden for the electric power industry. Additional changes to Form OE–417 clarify reporting criteria and allow respondents to select potentially applicable exceptions under the Freedom of Information Act for protection of the information provided within the submittal.

EEI supports the goals of the Department particularly aligning the new form with Reliability Standard CIP-008-6 and to reduce reporting burdens and offers the following comments to further enhance the clarity of the form.

The term “cyber event” was used on the OE-417 form prior to inclusion of the NERC CIP-008-6 Reliability Standard reporting requirements and NERC defined terms. However, the term “cyber event” is not a NERC defined term and could create confusion and consistency issues with reporting. For this reason, EEI suggests substituting the undefined term “cyber event” with the NERC defined term “Cyber Security Incident.”
EEI recommends the following changes to the form to better align with Reliability Standard CIP-008-6. The proposed revised form includes a section titled “Response Due” which details in what timeframe incidents must be reported. It states responses are due within 1 hour of an incident for a Reportable Cyber Security Incident (criterion 2) and a Cyber event that is not a Reportable Cyber Security Incident that causes interruptions of electrical system operations (criterion 3). EEI recommends that DOE modify this timeframe to be within 1 hour of the determination of the incident to align with the Reliability Standard CIP-008-6, Table 4, Part 4.2.

The Response Due section also requires “updates as needed and/or a final report (all of Schedules 1 and 2) within 72 hours of the incident.” This timeframe should be modified to align with Reliability Standard CIP-008-6. This requirement should state that a Reportable Cyber Security Incident (criterion 2) and an “attempted” Reportable Cyber Security Incident (criterion 14) are due within 7 calendar days of the determination of new or changed attributes to align with the Reliability Standard CIP-CIP-008-6, Table 4 Part 4.3.

In Section W of the proposed DOE-417 form, CIOCC is identified as one of the agencies to be notified in the event of a reportable Cyber Security Incident, while Reliability Standard CIP-008-6 identifies NCCIC as the appropriate Department of Homeland Security agency (DHS). As of June 2020, DHS established a new organization titled “CISA Central” to receive such reports. The revised OE-417 should be updated to reflect CISA Central rather than CIOCC.

EEI appreciated the Department’s consideration of these comments.