CONFIDENTIAL: FOR EEI AND AGA MEMBERS ONLY

Joint EEI-AGA Roundtable Discussion: Energy companies protection of employees and infrastructure during civil unrest
June 3 and June 5, 2020

EEI and AGA's Security Committees convened two conference calls on June 3 and June 5, 2020, to discuss what energy companies are doing to protect employees and infrastructure during civil unrest. The discussion was informative and valuable as energy companies face challenges from the civil unrest, as well as COVID-19, unemployment, and summer hurricane and wildfire season.

This summary is confidential and for information purposes only. The document or any of its contents must not be disclosed outside of your company. It is not intended to identify industry recommendations or best practices. The summary reflects these issues at a snapshot in time.

A summary of the observations and activities that were shared by roundtable participants include:

- Employee & Field Worker Safety
  - Employee safety is the number one concern, especially with the continued presence of COVID-19.
  - Used a security provider to hire off duty police officers. Directed employees to call the command center if they need an escort and then detail those officers to the employees.
  - Did not generally use escorts for morning activity. Later in the afternoon, considered only sending out employees when necessary for emergency calls AND with an escort.
  - Concern raised about the possibility police escorts could enflame the situation given present circumstances.
  - If protests are taking place near critical locations, considered staging field workers elsewhere so they don't have to be near the protests.
  - Considered requiring physical security leadership approval before sending employees out to conduct field work. Arranged for police escorts or support.
- Facilities in protest hotspots
  - Considered moving nonessential employees to an alternate location and moving control center to backup location, if necessary.
  - Built a plywood perimeter around first floor glass walls to prevent damage and looting.
  - Consolidated fire extinguishers in the event of fire (acknowledged local Fire Department may be overwhelmed).
  - Considered the likelihood of rioters using landscaping around the facilities as a weapon or to create damage (decorative stones and bricks, flowerpots, etc.).
  - Engaged with physical security alarm monitoring team to evaluate system.
- Security Guards
  - Considered keeping Security Guards inside of the building (rather than exterior to the building) for their safety due to potential targeting of any uniformed person.
  - Considered undercover/plain clothes security to observe direction/condition of protests.
  - Made sure there was an understanding around use of force, and at what point force would be exercised. This helps clear up confusion about how to respond to specific situations (e.g., where accelerants were being used by rioters to start fires).
- Internal Coordination

  - Using an enterprise-wide security approach – physical security, cybersecurity, and intel teams all play an important role.
  - Holding daily calls (suggested twice daily) to discuss threat intelligence, protests, impact to the company (road conditions, weather), security and operations activities.
- Engagement with local Police and Fire Departments
  - Recognized that local first responders may be overwhelmed and unable to respond immediately.
  - Noted police stations and police staging areas may become hotspots for protesters and rioters.
  - Sharing intelligence with local law enforcement for ground truth.
- Coordination with National Guard
  - Activated in 23 states as of 6/3/20.
  - Providing GIS locations of critical substations/facilities for protection.
  - Sharing available intelligence.
  - Discussing escort capabilities for essential work.
- Intelligence gathering and sharing
  - Sharing information with the DNG-ISAC and E-ISAC (and any others).
  - Opened communication channels internally and with other groups in the community to share real time information – WhatsApp® has been a tool for this.
  - Monitoring social media such as Twitter®, Facebook®, Instagram®, and Snapchat® heatmap for signs of organized messaging and activity – protests and supply stations (in some locations, people inciting riots were dropping off propane, lighter fluid, and gas)
  - Be aware nation state adversaries are actively engaged in disinformation campaigns online to inflame, incite, and encourage strife and division. Validating as much information as possible before acting.
  - Monitoring local radio programs, or camera feed sharing programs such as MutualLink®.
  - Monitoring and sharing information regionally to determine what security protection plans may be necessary.
  - Sending a company liaison to the State Emergency Operations Center (EOC) if activated.
  - Applying *User and Entity Behavior Analytics* (UEBA), an emerging technology from 2014 (started as User Behavior Analytics) that has gained more widespread use in the last couple of years and helps address two critical points in a Cybersecurity program. The first is the identification of anomalous and malicious activity that is a deviation of the normal baselines in the environment and the second is the identification of current or growing insider threats. There are numerous vendors in this space.
  - Observed signs of suspicious organized activity have included cars without license plates, groups walking/patrolling with personal firearms, strategically set fires, attempts to loot tires to create black smoke.