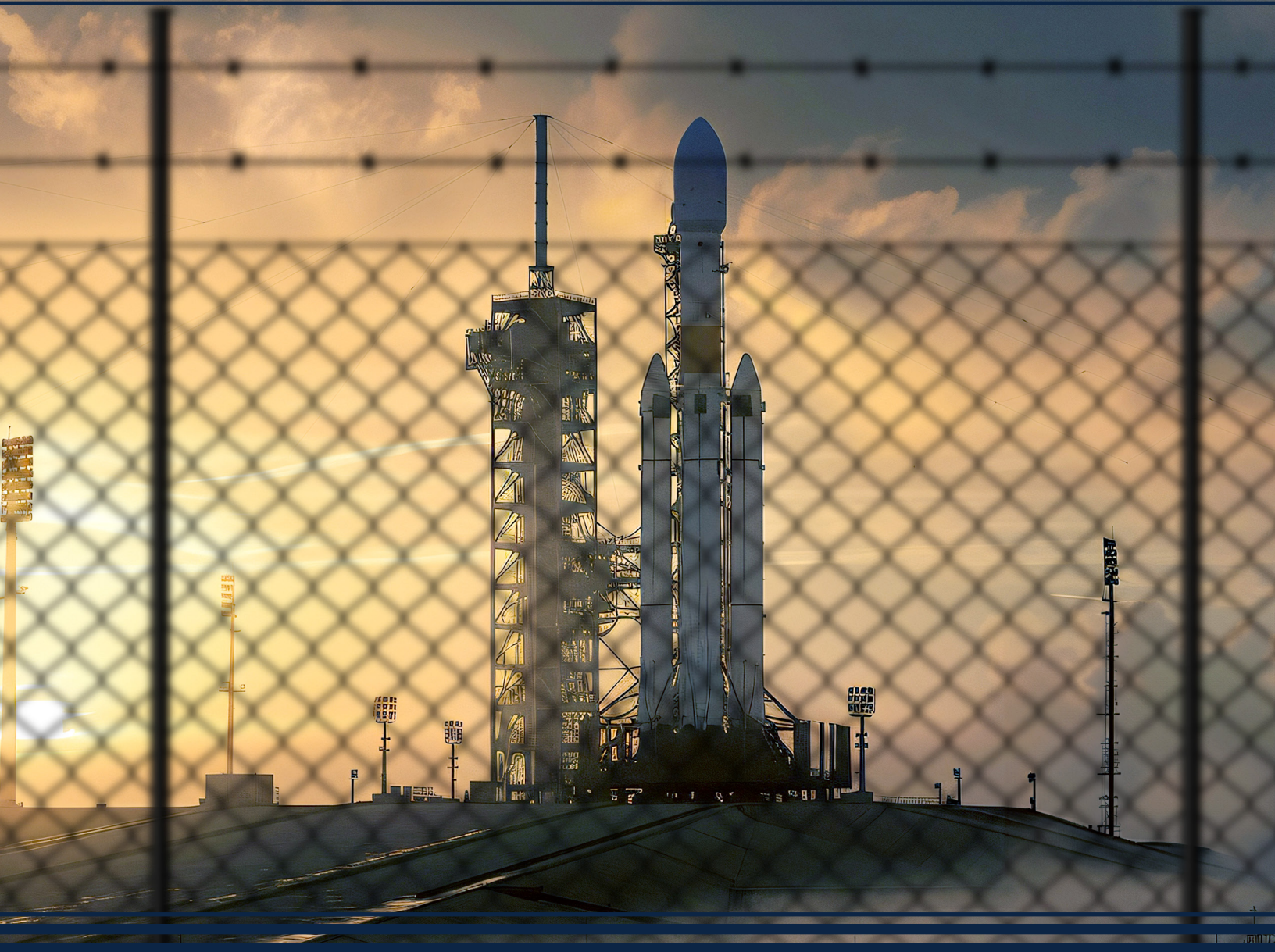
BEST PRACTICES FOR

SPACEPORT SECURITY



JULY 2024

Federa Av at on
Adm n strat on

Table of Contents

ACRONYMS

AOA Air Operations Area

CCTV Closed-Circuit Television

DIN Deutsches Institut für Normung[1]

ETD Explosive Trace Detection

ICC International Criminal Cartel

IDS Intrusion Detection System

IPS Intrusion Prevention System

MFA Multi-Factor Authentication

RFID Radio Frequency Identification

UPS Uninterruptable Power Supply

[1] German Institute for Standardization, the international standard for secure shredding of data media

Introduction

Spaceports provide essential infrastructure for the commercial space transportation industry. Comprehensive security measures should regularly be considered and implemented to mitigate risk to commercial spaceport operations. Limited scope security-related threat and vulnerability assessments (TVA) were conducted between January 2022 and March 2024 at multiple FAA licensed commercial spaceports by an interagency team which evaluated counterterrorism, counterintelligence, and cybersecurity risk. For purposes of this assessment, the following definitions were applied:

> *Counterterrorism* is defined as "incorporating the practice, tactics, techniques and strategy for businesses to counter potential terrorist acts against a facility or entity." (Derived from the DHS Strategic Freamework for Countering Terrorism and Targeted Violence September 2019).
>
> *Counterintelligence* is defined as "Information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons, or their agents, or international terrorist organizations or activities." (EO 12333, section 3.5(a)).
>
> *Cybersecurity* is defined by DHS CISA as "the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information." (CISA ST04-001).

This document contains best practice guidance, developed from the TVA process, for improving and maintaining physical and cyber security at commercial spaceports, as well as measures to protect against intellectual property theft and economic espionage. These recommendations are intended to build upon a foundation of collaboration between government agencies and private sector entities utilizing a layered approach towards security.

These commercial spaceport security recommendations are not exhaustive, regulatory, binding, nor meant to address site specific concerns. The TVA interagency team recommends commercial spaceport leaders consult with logical security professionals and regulatory authorities related to site-specific questions and security planning matters in their respective areas of operation.

Government and Private Sector Collaboration

US spaceports are owned and operated by governments (Federal, State, Local, Tribal) and private sector entities. Government leaders and homeland security agencies hold varied leadership positions to address specific security needs or issues and response related to spaceport activities. Like their government counterparts, private sector owners are responsible to conduct and execute business continuity planning, integrate security planning with disaster planning, and actively participate with Federal, State, Local, and Tribal governments to improve security in the space ecosystem. Commercial spaceport security strategies must be supported by a private sector that internalizes a strong security culture, embedding best practices and government requirements into day-to-day operations.

Commercial spaceport operators are encouraged to actively engage with US government and private sector stakeholders during planning processes and subsequent follow-up. Transparent and open dialog

between all stakeholders during planning efforts has proven vital for success and will increase effectiveness of risk mitigation actions and reduce burdens on the private sector.

Layered Security

Layered security is critical for deterring and preventing terrorist attacks, crime, cyber intrusion, economic espionage, protecting US space sector interests and intellectual property, combating insider threats, and mitigating damage and expediting recovery. Effective security utilizes active layered security and defensive measures that integrate public and private sector capabilities acting in concert and using diverse and complementary measures, rather than relying on a single solution.

At the minimum, a layered approach to commercial spaceport security means applying measures of security to areas including (but not limited to): personnel, physical site access controls, site deliveries, signage, foreign engagements, international travel, insider threats, tours/visitors, network/IT, and technology access controls.

Together, as one integrated system, layered security measures allow for resilience against expected and unexpected incidents. Each layer adds to security and in combination serves as a force multiplier. Layered security deters intended intrusions, operational compromise, and theft of intellectual property by continually disrupting a potential adversary's deliberate planning process.

Commercial Spaceport Security Planning Roadmap

The following recommendations are provided for use by commercial spaceport operators to support implementation and improvement of comprehensive security plans for spaceports already constructed and for those in planning phases. For additional resources, see security reference section at the end of this document.

1.0 Counterterrorism and Physical Security Recommendations

1.1 Personnel and Security Policies

- Hire a qualified Chief Security Officer responsible to set security policy and maintain security standards.
- Create comprehensive written security policies to set baseline requirements for site security and employee vetting.
- Ensure policies are available to employees and tenants and are regularly reviewed and updated as needed.
- Establish and maintain relationships with tenants and stakeholders, as well as local, state, and federal law enforcement agencies.
- Establish routine communication to share threat information covering criminal, counterterrorism, counterintelligence and cyber threats among tenants and stakeholders.

1.2 Control Access: Badging, Physical Security, Security Clearances

1.2.1 Facility Perimeter

- Construct and maintain a strong perimeter with a physical barrier, such as a fence with signs notifying potential intruders of boundary lines and limits.
- Consider utilizing lights and CCTV cameras along perimeter.
- Ensure entrances are marked and controlled to prevent unauthorized access.

1.2.2 Access Control

- Institute access points for personnel and vehicles through boundary lines such as gates, doors, electronically controlled or monitored access points.
- Minimize the number of access points and regularly monitor their use and condition.
- Consider random employee, visitor, and delivery vehicle searches.
- Escort non-employees, such as contracted custodial staff throughout the facility, to ensure protection of sensitive and proprietary information.

1.2.3 For Spaceports with a General Aviation facility on property:

- Keep Spaceport facilities separate from General Aviation facilities.
- When applicable, place signs and physical barriers on the AOA to delineate areas under control of the commercial spaceport operator vs. aerospace tenants vs. General Aviation facility and ensure tenants are aware of the boundaries.

1.2.4 Badging

- Establish multi-factor authentication capable (MFA) badging system covering the entire facility and require all tenants to use issued badges.
- Implement MFA card system with photo and biometric capabilities to ensure correct person is using the card. Modernize systems to track badge use and disable badges/cards when necessary.
    - Consider different colors for different tenants or access levels.
- Establish and document a robust badge accountability and audit process.
- Install closed circuit television (CCTV) cameras at all pedestrian/vehicle entry points to verify badge users' identity.
    - All videos should be recorded and stored for 30 days.
- Disable badges annually (or routinely if visit or contract is shorter) and require re-certification for employees and others who need long-term access, after a scheduled visit, or after an individual's work on a contract has ended.
- Ensure all employees are trained on proper security protocols for (1) security access badges and (2) reporting requirements for lost or stolen badges.
- Ensure tenants designate in writing a certification official - someone responsible for verifying the information of their employees and attesting to the employees need for access. The certifying official would ensure the employees are approved for access only to those areas needed for their position.

1.2.5 Additional Considerations

- Hire additional security for large events such as launches and demonstrations; or reassess contract security services to enhance capabilities and posture for reallocation of resources to critical areas around the spaceport.
- Consider implementation of static posts (gates and facility entrance) and random roaming patrols.
- Consider deployment of K-9 units as visible deterrents and to challenge suspicious bags, persons, and vehicles.
- Where possible, cross-train additional staff in security awareness procedures and concerns that will serve as force multipliers to identify and report suspicious activity.
- Acquire a document shredder to sufficiently destroy sensitive documents; should meet DIN 66399 standards for the material being destroyed (DIN P-3 through P-5).

1.3 Deliveries

- Physically screen and thoroughly examine all incoming goods before transfer into sterile areas.
- Utilize three or more layered countermeasures when physical screening of goods isn't feasible, to increase security of the sterile area-bound goods and better protect against contamination.
- Examples of countermeasures are:
    - Utilize X-ray and Explosive Trace Detection.
    - 100% physical screening (random or comprehensive)
    - Schedule deliveries.
    - Restrict deliveries to non-peak hours.
    - Utilize manifest for delivery confirmation.
    - Conduct periodic/random testing of the inspections process.
    - Use K-9 teams, as appropriate.
    - Plan off-site delivery: goods delivered to airside in smaller, recognized vehicles.
    - Conduct in-vehicle inspections before entering the airfield or facility for unloading, with goods staged in the vehicle.

1.4 Signage

- Regularly add, update, and upgrade signage so all communication needs are sufficiently met and maximize site safety. Replace and update signs when degraded.
- Place new and upgraded warning signs in appropriate locations around entire facility.
- Coordinate signage to appropriately draw attention and ensure style consistency with other signs whenever possible and appropriate.
- Construct signs of durable materials, using contrasting colors and reflective material where appropriate.

- Areas with access control or CCTV may have signage for directional, legal or law enforcement purposes. The signs should use the appropriate phrases as listed below:
    - "NOTICE: All activities in this area are being monitored and recorded."
    - "ALARM WILL SOUND IF OPENED"
    - "AUTHORIZED PERSONNEL ONLY"
    - "RESTRICTED AREA"

2.0 Counterintelligence Security Recommendations

2.1 International Partners and Foreign Engagements

- Develop standard operating procedures for foreign engagements such as routine business inquiries, joint ventures, collaborations, visitors to the site, tours, etc.
- Consult and coordinate with federal partners to determine if foreign interactions, business ventures, customers or foreign visitors to the facility pose a security risk.
- Negotiate strong nondisclosure agreements and joint venture terms with international partners and users of the spaceport.
- Develop plans to control and limit access to any sensitive information handled on site.
- Ensure cyber and physical security measures are in place and supported by policies and procedures to protect spaceport data.
- Identify all proprietary and sensitive information so the appropriate cyber and physical security measures can be enacted and enforced.
- Control and limit access to classified and sensitive info to protect against unauthorized disclosures.

2.2 International Travel

- Develop and implement consistent standards to protect employees, their devices, and spaceport data when traveling abroad.
- Conduct employee pre- and post-travel safety and informational briefings.
- Engage with federal partners for up-to-date threat and travel briefings.
- Provide loaner devices for international business travel.
- Scan devices for malware and sanitize electronics upon return.
- Encourage employees to keep identification, phones, and other electronics on them at all times during travel, and not access electronics given to them by others.

2.3 Insider Threat[2] Mitigation

- Develop relationships with federal partners to engage on counterintelligence matters.
- Develop and conduct annual counterintelligence and insider threat awareness briefings, in partnership with the FBI, to be provided to all current employees and new hires. Include state and county board of directors, spaceport authority boards and appointees, and other involved parties in the briefings.
- Develop an insider threat team to review and discuss potential issues. The team should consist of managers from information technology, legal, human resources, and security functions.
- Develop policies for photography, audio/video recording, social media posting or usage and communicate to all employees, interns, and visitors.
- Develop formal newly hired employee and intern vetting policy; consider including criminal and financial background checks, drug screening, verifying references, and non-disclosure and non-compete agreements upon hiring.

2.4 Tours/Visitors

- Develop written standard operating procedures and policies for visitors to the site and include:
    - Tour approval procedures
    - Vetting processes
        - Consider using security and export controls lists to screen such as Consolidated Screening List www.trade.gov/consolidated-screening-list.
    - Notification to employees
    - Require identification/badging at all times.
    - Provide instructions for visitors including - photography, audio and video recording, social media posting.
- Establish policies to control access and maintain security during tour group and visitor events at spaceport facilities.
- Establish policies to protect the physical safety all working on site during tours or other visitor events.
- Establish policies to protect exposure of sensitive work conducted by tenants during tours or other visitor events.
- Provide employee escorts for all visitors and tours to protect restricted access areas.
- Ensure positive access and on-site control is kept over tour groups and visitors to the spaceport; ensure groups are not shown or advised of sensitive tenants or sensitive work conducted by tenants.
- When co-located or adjacent to a federal facility consider coordination with federal partners to vet all visitors - including foreign nationals - visiting facility.

[2] The insider threat is an employee who has legitimate access to company information and provides that information to a foreign adversary. The steps herein may mitigate risk related to intentional and accidental insider threats.

3.0 Cyber Security Recommendations

3.1 Network/IT

- Create an IT Management Plan to protect the security of the network and the proprietary information transported.
- Utilize NIST or CMMC Cybersecurity Framework (CSF) Guidelines to assess, prioritize, and coordinate cybersecurity efforts to address and minimize cybersecurity risks.
- Update network diagrams to reflect current configurations.
- Systems should have its own firewall and intrusion detection systems (IDS).
- Systems should be physically or logically segmented and use separate firewalls and IDS/IPS to protect against unauthorized connections.
- Install IDS/IPS devices to detect man-in-the-middle/snooping on the transmission between microwave/Wi-Fi transmitters/receivers; Ensure proper encryption level for data.
- Provide separate wi-fi signals for tenants and cameras.
- Integrate device management on all issued devices.
- Create SOPs for disposing of electronic devices; physically remove outdated legacy systems or hardware no longer utilized on network to prevent reconnecting with malicious intent.
- Add additional system redundancies to the IT Management Plan such as:
    - Uninterruptable Power Supply (UPS) Systems
    - Back up data and file servers
    - Incorporating hardline phones in the event current VOIP phone systems become disabled.
    - Develop, implement, and biannually test a Continuity of Operations Plan (COOP).
    - Conduct annual penetration test assessments from outside and inside the network.
    - Conduct weekly vulnerability scans of networks.
- Seek increased IT funding and apply it towards upgrading critical components and legacy equipment.
- Consider adding additional employees (one or more) with IT networking and security backgrounds to the organization. Additional staffing will assist the IT dept in:
    - Continuing to upgrade the network infrastructure based on a maturity plan.
    - Provide additional customer and employee support and conduct maintenance in a timelier manner.
    - Provide more employees to handle dynamic network security incidents.

3.2 Access Control

3.2.1 Access Control as a Security Measure

- Implement and manage Access Control as an “air-gapped” system

- Segment Access Control systems from being able to access, or be accessed from, the public internet

3.2.2 Network Access

- Ensure all default usernames and passwords are changed on all networked devices - servers, routers, employee laptops and phones, etc.
- Should require users to utilize passwords with min 16 characters incorporating capital letters, lower-case letters, numbers, and special characters.
    - Should require personnel to change password on a regularly scheduled basis.
    - Prevent password reuse for a certain period.
    - Highly recommend incorporating multi-factor authentication (MFA) on any site-issued devices or other devices used on the site's networks.
- IT department should require everyone with direct network access - employees, contractors, anyone else - to sign a cyber-adherence policy, outlining rules for use of equipment and technology and keep records of the trainings: (1) employee cybersecurity awareness and (2) insider threat.
- Do not allow remote access onto systems without proper security procedures and segmentation of the security and observation systems.
- No remote access onto network without proper security measures in place - transmission encryption, MFA, logical and physical segmentation of system

3.2.3 Building Access

- Incorporate MFA control systems in private and sensitive areas.
- Establish policies detailing the level of access required for employees, contractors, and tenants; create access log reviews and audits to identify abnormalities and inactive accounts.
- Install intrusion alert systems on doors to sensitive areas that will alert security if the door is held open beyond specific amount of time to prevent tailgating or suspicious activities.
  Institute a badging policy requiring contract employees to check-in/out facility access badges daily and should not be taken off-site.

ADDITIONAL RESOURCES

1. The White House, *United States Space Priorities Framework*, December 2021: https://www.whitehouse.gov/spacecouncil/

2. US Department of Transportation, Federal Aviation Administration, Office of Commercial Space Transportation, Information and Resources: https://www.faa.gov/space

3. US Office of the Director of National Intelligence, National Counterintelligence and Security Center, Office of the Director of National Intelligence, Security and Counterintelligence Resources: https://www.dni.gov/index.php/ncsc-home to include *Safeguarding The US Space Industry, Keeping Your Intellectual Property in Orbit,* https://www.dni.gov/files/NCSC/documents/SafeguardingOurFuture/FINAL%20FINAL%20Safeguarding%20the%20US%20Space%20Industry%20-%20Digital.pdf

4. US Department of Defense, Defense Counterintelligence and Security Agency, Security and Counterintelligence Resources: https://www.dcsa.mil/

5. US Department of Defense, Chief Information Office, Cybersecurity https://dodcio.defense.gov/CMMC/About/

6. US Department of Defense*, National Industrial Security Program Operating Manual* (NISPOM) 32 C.F.R. Part 117 https://www.federalregister.gov/documents/2020/12/21/2020-27698/national-industrial-security-program-operating-manual-nispom

7. Defense Federal Acquisition Regulation Supplement (DFARS Subpart 204.73 —*Safeguarding Covered Defense Information And Cyber Incident Reporting, Scope and Definitions* https://www.acquisition.gov/dfars/subpart-204.73-%E2%80%94safeguarding-covered-defense-information-and-cyber-incident-reporting

8. US Department of Homeland Security, https://www.dhs.gov and DHS fact sheet to Help Businesses Plan, Prepare and Protect from an Attack: https://www.dhs.gov/sites/default/files/publications/Hometown-Security-Fact-Sheet-04062016-508.pdf

9. US Department of Homeland Security, Cybersecurity and Infrastructure Security Agency (CISA), https://www.cisa.gov; Cybersecurity and Infrastructure Security Agency, *Security Tip (ST04-001), What is Cybersecurity?* https://www.cisa.gov/uscert/ncas/tips/ST04-001#:~:text=Cybersecurity%20is%20the%20art%20of,integrity%2C%20and%20availability%20of%20information and https://www.cisa.gov/standards , and National Infrastructure Protection Plan and Resources: https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/national-infrastructure-protection-plan-and-resources

10. US Department of Homeland Security, Transportation Security Administration*, Security Guidelines for General Aviation Airport Operators and Users* https://www.tsa.gov/sites/default/files/2017_ga_security_guidelines.pdf

11. US Department of State, Directorate of Defense Trade Controls, International Traffic in Arms Regulations (ITAR), https://www.pmddtc.state.gov/ddtc_public/ddtc_public ; Understand ITAR https://www.pmddtc.state.gov/ddtc_public/ddtc_public?id=ddtc_public_portal_itar_landing Public Portal (state.gov)

12. US Department of Justice, Federal Bureau of Investigation, Counterintelligence https://www.fbi.gov/investigate/counterintelligence

13. US Department of Commerce, National Institute of Standards and Technologies (NIST), United States Department of Commerce, NIST SP 800-171 (NIST), 110 controls https://www.nist.gov/cybersecurity and https://www.nist.gov/cyberframework

14. US Department of Commerce, International Trade Administration, Consolidated Screening List https://www.trade.gov/consolidated-screening-list, and Bureau of Industry and Security Entity List https://www.bis.doc.gov/index.php/policy-guidance/lists-of-parties-of-concern/entity-list