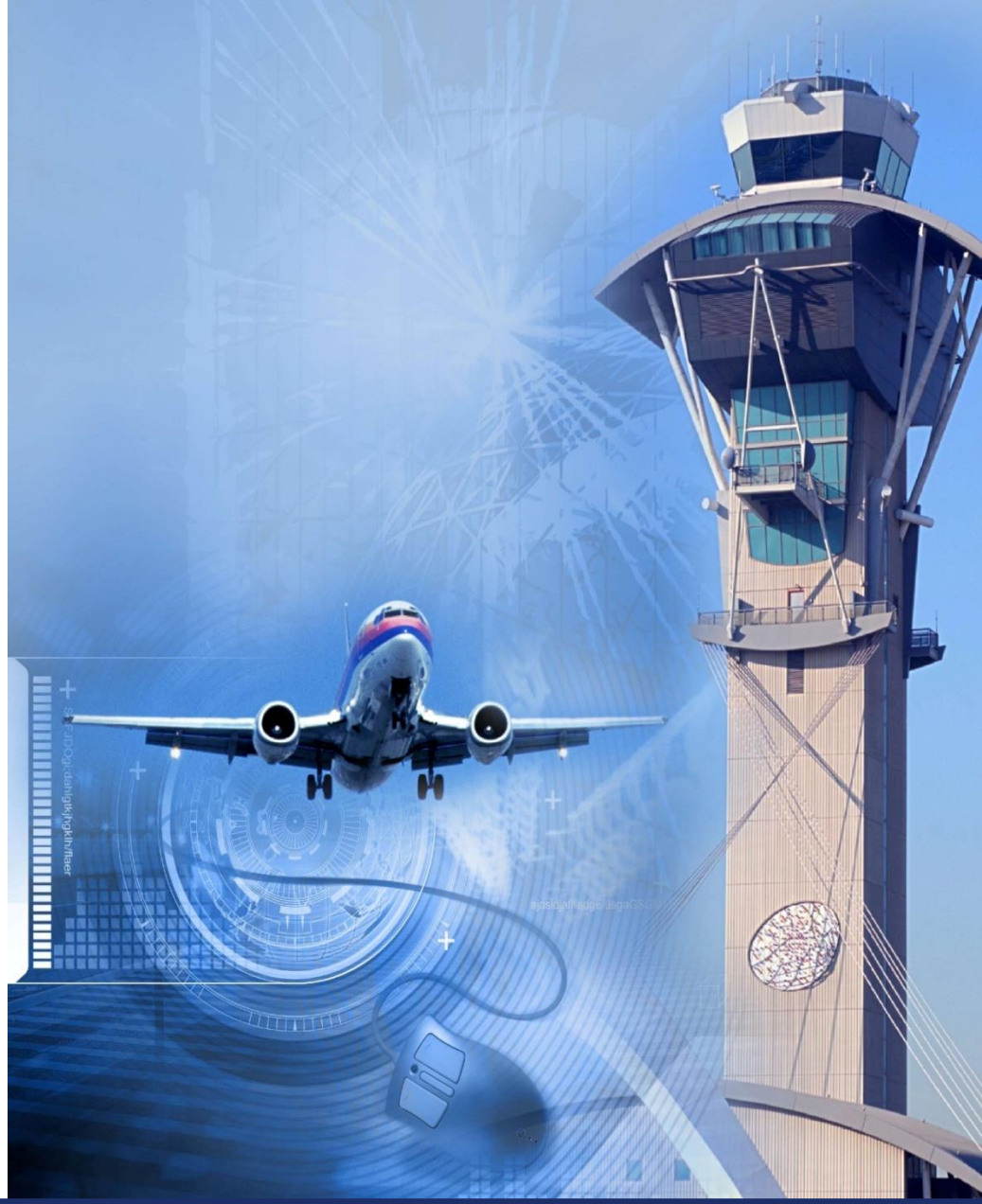
ACG

Data Calls and Responses

Program Control & Governance (PC&G)



July 2020

Federal Aviation Administration

Data Call Origination

- **Data calls may originate from many sources:**
  - DOT OIG:
    - As part of FY OIG Audit
  - GAO:
    - Response to GAO findings
  - FAA SOC:
    - Critical system/software issues
  - ATO NCO:
    - Critical system/software issues
  - DHS
    - Critical system/software issues
- **Some data calls are more critical than others and require immediate response**

Critical DHS Data Calls

- **Binding Operational Directives (BOD)**
  - A binding operational directive is a compulsory direction to federal, executive branch, departments and agencies for purposes of safeguarding federal information and information systems.
  - The Department of Homeland Security (DHS) develops and oversees the implementation of binding operational directives pursuant to the Federal Information Security Modernization Act of 2014.
  - Federal agencies are required to comply with DHS-developed directives.
- **Emergency Directives (ED)**
  - *Section 3553(h) of title 44, U.S. Code, authorizes the Secretary of Homeland Security, in response to a known or reasonably suspected information security threat, vulnerability, or incident that represents a substantial threat to the information security of an agency, to "issue an emergency directive to the head of an agency to take any lawful action with respect to the operation of the information system, including such systems used or operated by another entity on behalf of an agency, that collects, processes, stores, transmits, disseminates, or otherwise maintains agency information, for the purpose of protecting the information system from, or mitigating, an information security threat."*

Urgency of Response

- **Urgent responses are required based on:**
  - **Credible threat vectors based on National intelligence**

  - **Knowledge of actual vulnerabilities that may be exploited to access or control critical air transportation infrastructure**
  - **Vulnerabilities that have already been exploited**

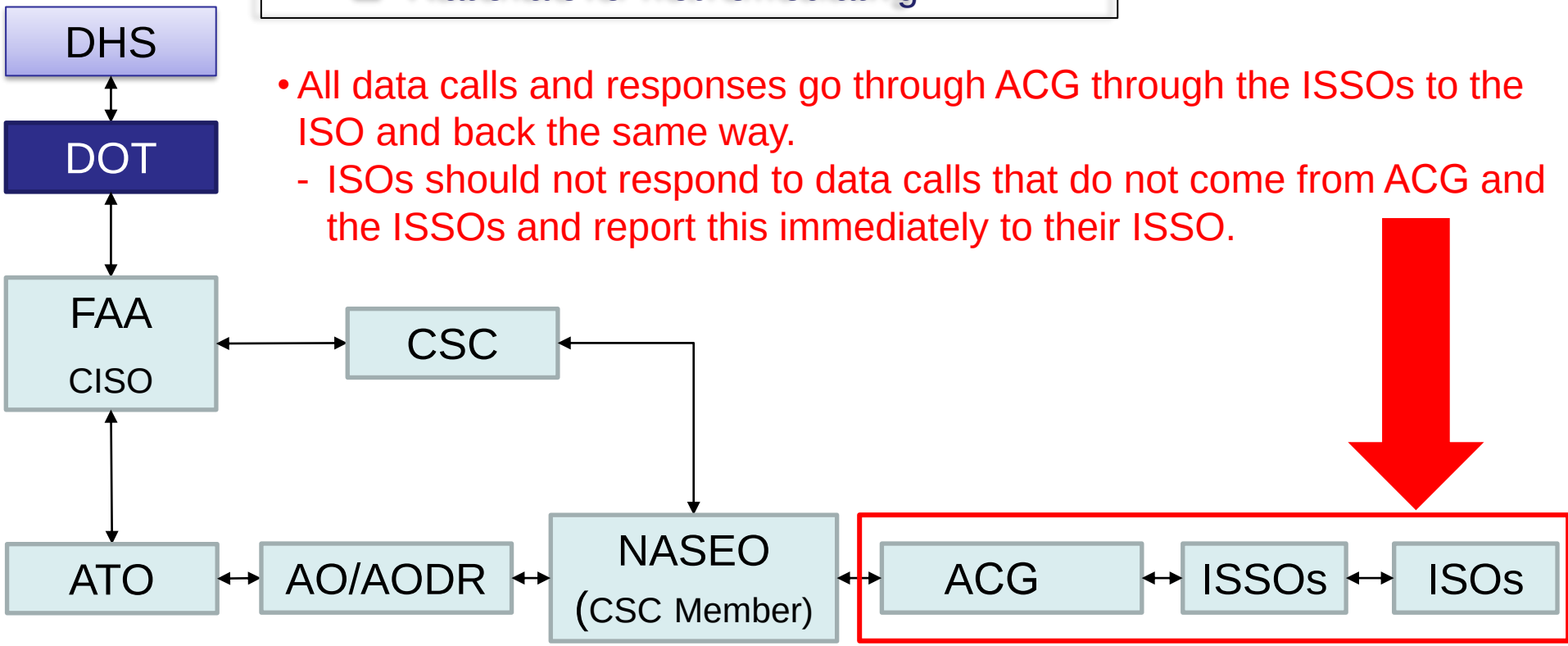
- **If an Emergency Directive indicates a patch or other remediation is needed, these patches are considered *Emergency Patching* and must be done immediately**

Data Call Process Flow

- **ATO monitors and reports critical data calls daily**
  - Cybersecurity Steering Committee and CISO notified of progress

- Process is tracked through completion
  - ❑ Progress against remediation
  - ❑ Rationale for not remediating

- All data calls and responses go through ACG through the ISSOs to the ISO and back the same way.
  - ISOs should not respond to data calls that do not come from ACG and the ISSOs and report this immediately to their ISSO.



Responses

- **Responses can be time consuming, but are important to maintain security of our ATO infrastructure and services**
- **Please do the following:**
  - **Submit responses by required due dates**
  - **If responses are delayed, please inform ISSO to pass “up the chain” with anticipated resolution date**
  - **If unable to remediate, please state rationale**
  - **If remediation is in progress, please provide an expected completion date and continue to report progress**
- **THANKS**

Conclusion

- **Critical data calls are based on credible threat information**
- **Rapid responses are key to maintaining up to date status on weaknesses in FAA infrastructure**
- **ISOs should only respond to data calls emanating from ACG through their ISSOs and report data calls that may come from other organization**
- **Your time and effort are greatly appreciated**