

## ORGANIZATIONAL EXCELLENCE

### Information Security



Federal Aviation  
Administration

#### FY 2008 Performance Target

*"Zero cyber-security events that significantly disable or degrade FAA services."*

#### Flight Plan Objective and Performance Target

**Objective 3:** Make decisions based on reliable data to improve our overall performance and customer satisfaction

**Performance Target:** Achieve zero cyber-security events that disable or significantly degrade FAA services.

	FY 2004 <sup>1</sup>	FY 2005	FY 2006	FY 2007	FY 2008
<b>Target</b>	90%	0	0	0	0
<b>Actual</b>	100%	0	0	0	

<sup>1</sup> The target for FY 2004 was the percentage of milestones achieved for FAA's information security plan.

#### Definition of Measure

**Unit of Measure:** Number of successful cyber attacks as determined by DOT/FAA's Cyber Security Management Center (CSMC).

**Computation:** A count of the number of successful cyber-attacks in the current fiscal year.

**Formula:** N/A

**Scope of Measure:** The measure is applicable to the DOT/FAA Information Technology assets, defined by TCP/IP systems, which contribute to the delivery of FAA services.

The FAA's information security infrastructure protects the agency's IT assets in accordance with numerous executive and legal requirements, including the Computer Security Act, Executive Order 13231, and the Federal Information Security Management Act (FISMA), as well as in accordance with DOT and FAA policy.

#### Why the FAA Chooses this Measure

Hackers seek to disrupt, or exploit critical infrastructure across the United States. One critical infrastructure, as identified by the President in Homeland Security Presidential Directive/ HSPD-7, is our transportation system, including aviation. Accordingly, the FAA, whose mission is to ensure the safe and efficient movement of aircraft, must be protected against the threat of cyber-attacks. The Office of Information Services (AIO) has the agency lead for ensuring that these attacks do not significantly disable or degrade FAA services.

#### Source of the Data

The data on cyber-security attacks are collected by the DOT/FAA Cyber Security Management Center (CSMC), which is part of AIO.

#### Statistical Issues

N/A

#### Completeness

The DOT/FAA's CSMC works collaboratively to validate cyber incidents on FAA and departmental systems. This process provides the most accurate and up-to-date measure. The FAA and DOT use current and historical data to validate trends, which indicate an increase in the number and complexity of cyber-attacks.

AIO has sensors on the DOT/ FAA's networks. AIO is the primary focal point of incident reporting to the DOT and USCERT.

**Reliability**

The DOT/FAA's CSMC collaborate with other ISS components in the federal government. The CSMC has the responsibility, as outlined in FAA Order 1370.82A, of being the focal point for all cyber incidents in the FAA.