

ISW 2001 Qualification Statement for Arthur Pyster
Federal Aviation Administration

arthur.pyster@faa.gov

202-493-4570 (voice)

202-267-5719 (fax)

Dr. Arthur Pyster is the Deputy Assistant Administrator for Information Services and Deputy Chief Information Officer for the Federal Aviation Administration. In that role, he is responsible for information security for all computers and information in the FAA, which controls the safe air travel of 2,000,000 passengers daily throughout the United States.

Over the past 2½ years, the FAA has conducted a major effort to upgrade its information security posture, including the establishment of information security policy, training, architecture, network monitoring, and the deployment of several hundred staff in various security roles. Most major information systems have now been assessed for security vulnerabilities, with mitigations now in effect for many of them. The agency is on track to mitigate vulnerabilities in all FAA systems that are part of the nations critical infrastructure as defined in Presidential Security Directive 63.

Historically, the FAA has prepared for attacks that could disable a small number of air traffic control (ATC) system elements. The ATC system is highly redundant and robust in the face of isolated equipment outage that results from either routine failure or from sabotage. Threats that could impact wide segments of the ATC system were effectively non-existent. With the movement of ATC systems to commercial components, much higher connectivity among ATC components, and greater reliance on IP-based services and the Internet, the potential for wider disruption in ATC services is higher. The most important focus of the information security program at the FAA is to understand and counter these new threats and to position the FAA to recover rapidly and minimize damage should such an attack ever take place.

The two questions I would like to see addressed at the workshop are:

1. How should a very large distributed safety-critical network be architected to allow the secure passage of information to and from less secure non-safety critical networks?
2. Under what conditions can safety critical and non-safety critical systems share communications and computing infrastructure so that a successful attack on the non-safety critical systems will not impact safety-critical systems?