CPNI
Centre for the Protection of National Infrastructure

CYBER SECURITY IN CIVIL AVIATION

August 2012

This is version 1 of this report, describing the situation as of August 2012, and the intention is to update it periodically as the situation changes. We welcome feedback on this report to correct errors and to develop it for use by the widest possible audience of civil aviation stakeholders.

Summary

This document is the work of the UK Centre for the Protection of National Infrastructure (CPNI), based on work done by the Joint Coordination Group (JCG)[1]. The JCG's objective is to coordinate activities associated with the development of cyber security for civil aviation, based on the views of the industry itself, and with input from other stakeholders.

A general rule for cyber security is that it should be implemented 'top-down' through direction as well as 'bottom up' through technology. The 'top' of the Civil Aviation control system is the International Civil Aviation Organisation (ICAO). As a result, ICAO needs to have appropriate measures and management strategies to implement, support and secure civil aviation, particularly the new 'eEnabled' aircraft[2] and the future Air Traffic Management (ATM) systems, being designed by the SESAR, NextGen and Carats projects. A single cyber security architecture will be required to enable these new systems to inter-operate seamlessly, securely, and safely worldwide.

The JCG considers the present situation to be critical, as eEnabled aircraft are increasingly coming into service and work on various ATM projects has started, with no agreed concept of the information security architecture that civil aviation will require in the future. Unless this situation improves soon this must inevitably lead to rework, redesign, delays and extra cost, and may result in less secure systems.

This report describes the situation that exists today, and identifies government and industry bodies which are currently involved. It also lists a number of recommendations derived from JCG internal discussions and discussions with ICAO concerning a potential ICAO Cyber Security Task Force.

It should be remembered that computer security is as old as computing, but has always been seen as a side issue. Calling it cyber security has not changed this fundamental position, but the cyber world of interconnected and interdependent systems has increased the vulnerability of aircraft and systems and therefore the potential impact that breaches in security can have. More attention is therefore due to this complex but containable problem.

[1] See page 14 for details of the JCG
[2] Boeing B787, Airbus A380 and A350, and similar

Contents

The situation today

Cyber security is an issue because many civil aviation organisations rely on electronic systems for critical parts of their operations, and for many organisations their electronic systems have safety-critical functions. The protection of electronic systems from malicious electronic attack and dealing with the consequences of such attacks is encompassed by the term ‘cyber security’. It comprises managerial and technical activities, and relates to the electronic systems themselves and to the information held and processed by such systems.

There are a number of reasons why risks to civil aviation from malicious cyber activity are increasing. These are explained in more detail in the sections below but can be summarised as:

- Safety vs security – There is a widespread opinion that safety management deals with all security issues, but since safety management discounts malicious activity then this is not the case;
- New technology and lack of experience – Much of the new IT technology being introduced raises potential security issues which are unfamiliar in the civil aviation industry;
- Consolidation – IT systems are becoming increasingly interconnected and interdependent, so organisations are exposed to risks caused by security weaknesses in other people’s systems.

Control of aircraft in airspace

Today air traffic is controlled using instructions issued from the ground by radio, with aircraft position determined by radar, and things have not substantially changed for 70 years. With increasing air traffic (see estimates from the SESAR and NGATS projects) today’s system is beginning to hit its physical limits, particularly in terms of the number of aircraft that can be managed by human controllers within a given airspace. The industry has designed solutions to automate the routine part of air traffic management, which if put into place, would greatly increase the number of aircraft that can be managed within a given airspace. This would leave the air traffic controller with the ‘executive’ role rather than having to issue all the ‘routine’ control instructions, which would be produced automatically by the system.

The expected widespread use of Unmanned Aerial Vehicles (UAVs) in the near future also raises new issues due to the increased importance of remote linkages and ground control stations.

These and other air traffic control issues are being solved by the introduction of new communication methods and technologies, which includes the use of internet based solutions. The use of these increases the role of cyber security and exposes numerous vulnerabilities that do not exist in today’s more ‘closed’, proprietary, civil aviation

systems. These cyber security vulnerabilities have the potential **to jeopardise civil aviation safety and efficiency.**

Aircraft manufacturers

Developments in aircraft design have been more radical than those in ATM, at least in terms of the use of Information Technology to manage and control aircraft. The latest aircraft rely on interconnected systems which extend off the aircraft to ground-based systems run by airlines, airports and Aviation Service providers of various types. Manufacturers have introduced 'Commercial Off-The-Shelf' (COTS) software and hardware into the aircraft as part of the new systems aboard, with the objective of driving down costs and speeding development times. This also adds potential security risks, since vulnerabilities and weaknesses of the new technologies are well understood by a larger number of malicious actors.

Aircraft manufacturers have also developed systems that permit communication of all the routine air traffic commands between air traffic control and the aircraft that use these new technologies. These systems are being used in commercial service, but for security reasons, the pilot has to feedback, via radio, the command he is requested to execute by the system. Thus the solution itself raises a fundamental security problem, and adds to the radio traffic.

Taken together, these developments mean that the latest aircraft have a potential for cyber vulnerabilities that previous aircraft did not, which **could jeopardise civil aviation safety and efficiency.**

Aircraft operators

Aircraft operators (both commercial and military) wish to make use of the new communications capabilities to support their missions, develop new cost efficient operations and maintenance procedures, and offer new revenue producing services. These intentions can only be realised by moving more information on and off the aircraft on a regular basis, which also introduces a number of vulnerabilities that can be exploited by a cyber attack, which have **the potential to jeopardise civil aviation safety and efficiency.**

Rule-making and regulatory bodies, the industry, direction and leadership

The rule-making and regulatory bodies are struggling to provide the certification criteria, methods and toolsets which will be required to substantiate the airworthiness assurance, i.e. safety, related to the new cyber security dimension. This applies equally to the manufacture, operation and maintenance of the new aircraft and new ATM systems. Risks are increased by the increased use of internet technologies and COTS systems both 'on' and 'off' the aircraft.

A significant number of related initiatives, projects, programs and activities are currently underway to solve various portions of the issue, but there is no general

overall coordination of these related efforts. The industry is ardently seeking direction and leadership from the governance and government bodies (ICAO, FAA, EASA, EU, ECAC, etc.).

Governments and CAAs are struggling to get to grips with these issues in ways that promote security, safety and efficiency. They frequently suffer from a lack of expertise and experience in these areas which are difficult to remedy in the short term. Oversight and coordination by a recognised global authority is necessary to ensure a viable

resolution, facilitate the cost-effective use of limited resources (both in terms of people and funds) and resolve any parochial issues. To be fully effective, the solution for this situation must be globally applicable.

Further difficulties: The 'Connexion by Boeing' experience

Boeing created a company in the early 2000s whose business objective was to integrate internet access into commercial aircraft. Routing technology was installed in the aircraft and the entire aircraft was given IPv4 public routable internet addresses which were issued by an internet registry serving the airline's flag country. In flight, these aircraft were connected directly to the internet via KU band satellite linked to a ground station that had direct internet connections. As the aircraft flew on longer international or trans-oceanic flights, they would pass out of one satellite's coverage area into another's, connected to a new ground station literally on another side of the globe. In order to keep the passenger's internet connections from being dropped during this handoff between satellites, Connexion would dynamically withdraw the aircraft's assigned IP network from one region's ground station and insert them in the new region's ground station. Here, they unknowingly created what became a major technical problem for routing technology.

As these aircraft routers were reconnected at their new ground station on a different continent, significant amounts of internet traffic were generated by routers automatically updating their tables of addresses. Just as Boeing was closing down Connexion in late 2006 for commercial reasons, they were informed that in the future the internet would block this movement of aircraft routes between continents to preserve internet stability. Thus this method of connecting aircraft as 'mobile nodes' to the internet had to be abandoned until a better method of managing the general problem of mobility could be found.

In late 2008, ICAO, the FAA, Eurocontrol, and other members of the aviation industry met with internet representatives from the Internet Engineering Task Force (IETF), which writes the standards governing the internet, the ICANN board of directors which governs part of the internet infrastructure, and the internet registries which distribute and govern internet address allocation and assignment. As a result of this meeting, several potential solutions to the aircraft mobile routing problem were identified. The IETF's MEXT, DMM, and other working groups have been at work on this problem with the Aerospace industry ever since, without yet achieving a solution.

Given that the basics of internet functionality are still to be resolved, there can be little confidence that all the security implications of eEnabled aircraft are being correctly identified and, where necessary, resolved.

The organisations involved

ICAO

The International Civil Aviation Organisation (ICAO) was set up by international treaty in 1944, and is an agency of the United Nations. To quote the founding convention on the purpose of ICAO (emphasis added by CPNI):

> *WHEREAS the future development of international civil aviation can greatly help to create and preserve friendship and understanding among the nations and peoples of the world, yet its abuse can become a* ***threat to the general security****; and*
>
> *WHEREAS it is desirable to avoid friction and to promote that co-operation between nations and peoples upon which the peace of the world depends;*
>
> *THEREFORE, the undersigned governments having agreed on certain principles and arrangements in order that international civil aviation may be developed in a* ***safe*** *and orderly manner and that international air transport services may be established on the basis of equality of opportunity and operated* ***soundly and economically****;*
> *HAVE accordingly concluded this Convention to that end.'*

ICAO is controlled by individual sovereign states, so it is a country forum, not an industry forum. Its council adopts standards and recommended practices based on the recommendation of the Air Navigation Commission. The support of industry in the development of SARPS is welcomed.

The use of standards and best practices (from ICAO web site)

> Twenty-four hours a day, 365 days of the year, an aeroplane takes off or lands every few seconds somewhere on the face of the earth. Every one of these flights is handled in the same, uniform manner, whether by air traffic control, airport authorities or pilots at the controls of their aircraft. Behind the scenes are millions of employees involved in manufacturing, maintenance and monitoring of the products and services required in the never-ending cycle of flights. In fact, modern aviation is one of the most complex systems of interaction between human beings and machines ever created. This clock-work precision in procedures and systems is made possible by the existence of universally accepted standards known as Standards and Recommended Practices, or SARPs. SARPs cover all technical and operational aspects of international civil aviation, such as safety, personnel licensing, operation of aircraft, aerodromes, air traffic services, accident investigation and the environment. Without SARPs, our aviation system would be at best chaotic and at worst unsafe.

ICAO has been working on SARPS for Air Traffic Network (ATN) security for a number of years and cyber security is now being addressed by these efforts. Also in the past ICAO has used SARPS to specify the telecommunication traffic and other services facilities needed to operate civil aircraft between countries. As these services are now migrating onto the internet for reasons of cost, ICAO is faced with a growing number of problems:

- The internet is regulated internationally by bodies such as the Internet Engineering Task Force (IETF) and Internet Corporation for Assigned Names and Numbers (ICANN), not individual nation states.
- The attitude within ICAO is that each state decides what telecommunications pass through their territory, and that they alone will be responsible for security. In a world where traffic, data, voice, video, etc. is transmitted via internet, this attitude is untenable in the long term.

ICAO has recently amended Annex 17 to include the information security dimension. Chapter 18 is being drafted as advisory material to member states. The ICAO Threat and Risk Working Group has developed and applied a methodology to evaluate malicious risks to civil aviation to inform amendments to Annex 17. That work has started to embrace emerging threats such as cyber attack.

ECAC

The European Civil Aviation Conference (ECAC) is an inter-governmental organisation of 44 European member states. It is an integral part of the ICAO global air transport family and deals with all aspects of civil aviation in particular in relation to safety, security, the environment, airspace, and economics. It seeks to harmonise civil aviation policies and practices amongst its member states, and to promote understanding on policy matters between its member states.

ECAC has a study group on cyber threats to aviation security that is writing guidance material for member states on cyber security control measures. This is in support of the mandate on ‘cyber threats to aviation’ in the recent chapter 14 of ECAC’s DOC30. Once the guidance material has been published it will be up to individual states to ensure it is followed by operators and organisations under the control of that state.

EUROCONTROL and SESAR

EUROCONTROL is an international organisation with 39 member states, supporting its members to achieve safe, efficient and environmentally-friendly air traffic operations across the whole of the European region. It not only manages day-to-day operations of the European Air Traffic Management (ATM) network, but also manages crisis situations. Eurocontrol has a major role in defining the future of ATM systems in the Single European Sky ATM Research programme.

There is no agreement yet on what regulation would be needed in future and how much should be mandatory. However, the principle advocated in SESAR was that security regulation is subject to subsidiarity:

- Central mandatory regulation should only be used to meet requirements for ATM security which cannot be effectively achieved by voluntary means, by uncoordinated action, by industry standards or guidance material.
- Existing regulations may need to be strengthened to meet the security vulnerabilities in the new, harmonised, integrated ATM system in Europe.

The Security Team (SET) is a EUROCONTROL advisory body, providing a direct channel of consultation between all stakeholders involved on activities pertaining to the security of air navigation. It comprises Eurocontrol employees, representatives from national air navigation service providers and regulatory bodies, and others with an interest in ATM security. The mission of the SET is to drive improvements in the management of threats and risks in the context of ATM security and the security of air navigation.

FAA and NextGEN

The Federal Aviation Authority, an agency of the United States Department of Transportation, has the authority to regulate and oversee all aspects of civil aviation in the U.S. It considers that new aircraft 'architectures and network configurations, may allow the exploitation of network security vulnerabilities if suitable protections are not in place to prevent the intentional or unintentional destruction, disruption, or degradation of data, systems, and networks critical to aviation safety. The existing part 25 regulations do not address these potential network security vulnerabilities that can be exploited by unauthorised access to aviation data networks. The FAA has been issuing special conditions to ensure that security, integrity, and availability of the aircraft systems and data networks are not compromised by certain wired or wireless electronic connections between airplane data buses and networks. Based on current industry trends, the FAA and industry are likely to face more challenging cyber-security issues.'[3]

NextGEN is the Next Generation Air Transportation System, a transformative change in the management and operation of how aircraft fly in the USA. It is an equivalent of the European SESAR project. NextGen enhances safety, reduces delays, saves fuel and reduces aviation's adverse environmental impact. The FAA has acknowledged that with the introduction of NextGEN systems and the move from closed to open systems the cyber-security risks will increase.[4]

Air Traffic Management systems in the USA are run by the FAA and their cyber security is governed by the Federal Information Security Management Act of 2002 (FISMA) which mandates the use of FIPS 199 and FIPS 200 to categorise the criticality of information systems and the level of security controls they require.

[3] Source FAA Transport Certification Update, Edition 30, Fall 2011
[4] Speech by Michael Huerta, to the IT/ISS conference, March 15, 2011

ARINC and AEEC

ARINC was established in the United States in the 1920's to manage radio communications for the Federal Communications Commission. The Airlines Electronic Engineering Committee (AEEC) was formed in 1949 to assist the industry in capitalising on the explosive growth of aviation electronics - or avionics - onboard aircraft. For the aviation industry today ARINC standards regulate the design, form and fit of aircraft systems, equipment and software to achieve interchangeablility, commonality and reduced costs for operators.

ARINC issued Report 811 'Commercial Aircraft Information Security Concepts of Operation and Process Framework' in 2005. Its purpose is to facilitate an understanding of aircraft information security and to develop aircraft information security operational concepts. This document also provides an aircraft information security process framework relating to airline operational needs that, when implemented by an airline and its suppliers, will enable the safe and secure dispatch of the aircraft in a timely manner. This framework facilitates development of cost-effective aircraft information security and provides a common language for understanding security needs.

AEEC NIS - (Network and Infrastructure Security) subcommittee

The scope of NIS is to harmonise network-related and security-related activities of the various AEEC subcommittees working in related areas. NIS serves as a focal point for liaison to groups external to AEEC in order to coordinate work in these areas. NIS will focus on the interfaces and not on the hardware or software applications. NIS will provide support to AEEC by providing operational assessments of networking and security issues.

NIS has coordinated the use of ATA Spec 42 standards within the AEEC subcommittees.

A4A (formerly ATA)

Airlines for America (A4A), formerly known as Air Transport Association of America, Inc. (ATA), was the first and remains the only trade organisation of the principal U.S. airlines. For over forty years, the commercial aviation industry has worked together through a joint international effort to establish specifications for improving business processes and information exchange.

Administered and published by the Air Transport Association (ATA) e-Business Program, these international specifications have evolved to meet the changing needs of the industry and to embrace the latest technological advances in information exchange.

The ATA Digital Security Working Group

The first meeting of what became the 'Digital Security Working Group' (DSWG) was held in Toulouse in July 1999. The rationale behind the industry setting up the group was that digital security was a complex matter, would become essential within the aerospace industry, and that, as a result, industry standards were required. Over the years the ATA DSWG has defined and developed what has become ATA Spec 42, and is now incorporated into the relevant ARINC standards for aircraft systems. ATA Spec 42 is the civil aviation industry's interpretation of IETF Public Key Infrastructure (PKI) RFCs (also known as ITU-T X.509). ATA Spec 42 is now used as the PKI standard in all ATA, ARINC, EUROCAE and RTCA documentation.

CEN – European Committee for Standardisation - TC 377

The objective of CEN/TC 377 is to prepare European Standards on subjects relating to the European Air Traffic Management Network. The Technical Committee (TC) will have a special focus on European standards under mandates given by the European Commission to the ESOs in support of the Single European Sky (SES) framework, and in particular in accordance with Article 4 (1) of the Interoperability Regulation ((EC) 552/2004) concerning community specifications. It will cooperate with the EUROCAE, EUROCONTROL, EASA (European Aviation Safety Agency) and ensure liaison with ETSI on telecommunication-related subjects and with other stakeholders as appropriate.

The TC377 Working Group 1 has produced a draft standard which extends ISO27001 to civil aviation. Called 'Air Traffic Management — Information security for organisations supporting civil aviation operations' it is designed for use by all civil aviation organisations. It specifies what to do in order to have an Information Security Management System which implements security measures, but does not say what should be done in detail. It also does not say how to do this in detail, nor does it specify how effective the ISMS should be. Effectiveness could be assessed using further standards in the ISO27000 family.

ETSI - the European Telecommunications Standards Institute

ETSI produces globally-applicable standards for Information and Communications Technologies (ICT), including fixed, mobile, radio, converged, broadcast and internet technologies. ETSI supports various transportation domains with standardisation activities which are carried out by key industry players and therefore reflect true market demand.

A major development area is Intelligent Transport Systems (ITS), which add information and communications technology to transport infrastructures and to all types of vehicles in an effort to improve their safety, reliability, efficiency and quality. They also help to optimise transportation times and fuel consumption, thus providing greener, safer and more economical transportation. Knowledge of exact geographical

locations is important to all these services, so the standardisation of Global Navigation Satellite Systems (GNSS) such as GPS and Galileo also plays a vital role. Furthermore, the combination of communications and services can lead to smart handling such as in the eFreight and the Single European Sky (SES) initiatives.

In aviation, ICT is gaining an increasingly important role. Applications such as air traffic control systems and services for passengers, e.g. on-board telephony and internet access, are specified by ETSI. In addition, ETSI supports the Single European Sky initiative which aims to replace the traditional, highly fragmented air traffic control structures within Europe by means of greater harmonisation and an assured interoperability.

ETSI has an industry specification group on Identity management for Network Services (INS).

EUROCAE - The European Organisation for Civil Aviation Equipment

The EUROCAE is an organisation that provides a European forum for resolving technical problems with electronic equipment for air transport. EUROCAE deals exclusively with aviation standardisation (airborne and ground systems and equipment) and related documents as required for use in the regulation of aviation equipment and systems. Membership exclusively comprises aviation stakeholders made up of manufacturers (aircraft, airborne equipment, ATM systems and ground equipment), services providers, national and international aviation authorities and users (airlines, airports and operators) from Europe and elsewhere. EUROCAE documents are widely referenced as a means of compliance to European Technical Standard Orders (ETSOs) and other regulatory documents.

As well as detailed test specifications EUROCAE also produces system performance (minimum operational performance standards) and guidance documents together with RTCA, Inc. EUROCAE also works with SAE in the United States. The joint effort allows for a single definition of a given technology in areas where there is little choice to another approach, for example in aerospace EUROCAE documents are also produced in the context of the applicable ICAO standards and are coherent with existing ARINC specifications to ensure global interoperability.

Working Group 72 - Aeronautical Systems Security

EUROCAE documents are developed by Working Groups (WG) composed of specialist scientists and engineers representing member organisations of EUROCAE and RTCA, and invited organisations. Working Group 72 has been formed to develop guidelines to address security concerns for aeronautical systems. From the WG-72 work on the cyber security of systems on the aircraft itself, the group has come to realise that all the other supporting information systems that are connected to the aircraft also have to be secured to the appropriate level necessary to achieve the 'total system' security and safety required. Therefore WG-72 is also seeking to establish standards that cover ground-based systems which could affect the safety of flight. This could include airline, airport and ATM systems.

RTCA SC 216

RTCA Inc. is a US volunteer organisation that develops technical guidance for use by government regulatory authorities and by industry. RTCA is sponsored as a Federal Advisory Committee by the US Federal Aviation Administration. Guidance documents are developed and drafted by Special Committee (SC) and are based on a consensus developed within the SC charged with responsibility for the given document. Despite the loosely defined requirements of membership in RTCA, the guidance documents are based on expert technical opinion. Although RTCA is sponsored by the US DOT FAA, RTCA is not an agency of the United States government, and hence the documents it publishes are treated as guidelines, not as requirements.

Special Committee 216 - Aeronautical Systems Security

SC-216 will work jointly with EUROCAE WG-72 to develop two documents - 1) *Minimum Aviation System Performance Standards (MASPS) for Aeronautical Electronic and Networked Systems Security*, and 2) *Security Assurance and Assessment Processes and Methods for Safety-related Aircraft Systems.* The committee's recommendations and guidance material should help ensure safe, secure and efficient operations amid the growing use of highly integrated electronic systems and network technologies used on-board aircraft for CNS/ATM systems and air carrier operations and maintenance.

Internet Corporation for Assigned Names and Numbers (ICANN)

ICANN was formed in 1998. It is a United States based not-for-profit public-benefit corporation with participants from all over the world dedicated to keeping the internet secure, stable and interoperable. It promotes competition and develops policy on the internet's unique identifiers. ICANN does not control content on the internet, nor does it manage access to the internet, but through its coordination role of the internet's naming system, it does have an important impact on the expansion and evolution of the internet.

The Internet Engineering Task Force (IETF)

The mission of the IETF is to make the Internet work better by producing high quality, relevant technical documents that influence the way people design, use and manage the Internet. The IETF pursues this mission in adherence to the following cardinal principles:

Open process - any interested person can participate in the work, know what is being decided, and make his or her voice heard on the issue. Part of this principle is the commitment to making the documents, the working group mailing lists, the attendance lists, and the meeting minutes publicly available on the internet.

Technical competence - the issues on which the IETF produces its documents are issues where the IETF has the competence needed to speak to them, and the IETF is willing to listen to technically competent input from any source. Technical competence also means that IETF output ought to be designed to sound network engineering principles.

US Department of Transportation (DOT)

The US DOT has a fundamental interest in a secure air transportation system. It cooperates with the FAA and the RTCA SC-216 work. Much of this is being done through the John A. Volpe National Transportation Systems Center.

The involvement of regulators

The FAA has been part of the RTCA SC-216 effort from the beginning. The equivalent European organisation EASA (European Aviation Safety Agency) is taking an interest in the work of EUROCAE WG-72. The Dutch and UK CAA national aviation safety agencies are also contributing.

The Joint (Industry) Coordination Group (JCG)

Due to concern in the civil aviation industry that the technical and business impacts of cyber security solutions were not understood or not being addressed, in early 2006 the ATA DSWG and the AEEC set up an informal group to work on this topic. The group members came from the AEEC, ATA, FAA, EUROCAE, and US DOT, and became the ‘Joint Coordination Group’. IETF have presented their work at one meeting, and contacts have been made with IATA. Members of the group have also assisted at some ICAO meetings.

The JCG had a total of 3 meetings during 2007 and 2008, and produced 3 white papers. After a 3-year lapse the JCG met again in late 2011, and in early 2012. ICAO assisted at the latter JCG meeting, and given their lack personnel with the required cyber experience, ICAO suggested the creation of a Task Force based on Industry

participation, to assist them to initiate improvements to cyber security. The JCG is thus working on this suggestion, and will present proposals to the ICAO Air Navigation Conference in November 2012.

The JCG feels that industry is looking for general direction and leadership to be set both by Governments and ICAO. If appropriate 'top-down' information system security is to be put into place the outlines have to be put into place and overseen by ICAO. The general directions JCG would like to see adopted are detailed in the proposals below. Industry would like to see assistance and support from ICAO member states to get the appropriate changes carried out.

Industry proposals

Industry would like governments to:

1. Create the awareness of the general cyber security threat.
2. Address the total 'Aviation System' cyber security problem going beyond the boundaries of the civil, military and space systems.
3. Regulate with industry to see that appropriate operational safety and security levels are set, obtained and maintained.
4. Collaborate with other national infrastructure cyber security and anti-terrorist organisations to facilitate the efficient communication of cyber security threat information and enable these to be addressed in a coordinated manner.

Industry would like ICAO to:

5. Create an ICAO Cyber Security Task Force (CSTF) to work with and across most, if not all, of the existing ICAO committees and the nation state members. It is considered that a top-level body is necessary to cover all aspects of civil aviation security (information systems, procedures and processes, information & network security architecture and the related physical security) as more and more critical air navigation, control and business information becomes transmitted using the internet and internet technology. The CSTF should work with the chairmen and participants of the various cyber security initiatives discussed in this working paper to:
    - understand to what extent their activities will contribute to the achievement of the global cyber security strategy;
    - identify any inconsistencies between the initiatives;
    - identify any inconsistencies between the strategy developed and the work being undertaken.
6. Address the problem of 'Worldwide' versus 'Nation State' regulation, at least as far as network implementation guidance, information security and internet matters are concerned.
7. Support an overall 'Civil Aviation Security Architecture' to enable e-Enabled aircraft and new air traffic control projects to inter-operate seamlessly, safely and securely.
8. Define requirements for the core internet architecture, naming standards, addressing, routing, and other network services to be used by the new advanced air traffic management networks as standardisation of these is necessary both for aircraft to operate globally and for a full security architecture to be developed.

9. Provide the resources to allow the ACP to make requests to ICANN for i) specific civil aviation IPv6 industry ‘Critical Infrastructure’ address ranges and ii) private or unique domain names.
10. Provide the resources to allow the ACP to work with the IETF to develop the changes to internet features that will be required for civil aviation to ensure that aircraft global mobility presents no risks to the internet core infrastructure.
11. Create and develop cyber security SARPS that would regulate and manage the new processes and rules being developed to govern the operation and maintenance of those information systems that run on, or support the aircraft, in the ground or the air. Recognise that these supporting systems have become part of the ‘airworthiness’ dimension and that they must be capable of allowing almost real-time responses and changes to protect aircraft against new and/or previously unknown threats.
12. Understand that cyber security technologies will evolve and will constantly require to be updated both in the air and on the ground.

Industry should:

1. Adopt a risk managed approach to cyber security.
2. Ensure that, from the start, any new systems and services fit the global cyber security architecture as it develops.
3. Carefully consider how any ‘new services’ introduced by any new products are to be implemented and maintained securely over the complete life cycle of the system.
4. Consider the security impact of retrofitting ‘new services’ to existing aircraft.
5. Carry out independent, formal, closed area, robustness testing (pen testing) of critical architectures, systems and services.
6. Provide training on information/cyber security to all relevant staff.