Naval Information Assurance Center (NIAC): An Approach Based on the Naval Aviation Safety Program Model[1]

Dr. Raymond J. Curts, CDR, USN (Ret.)
Dr. Douglas E. Campbell, LCDR, USNR-R (Ret.)
Syneca Research Group, Inc. (www.syneca.com)
P.O. Box 2381, Fairfax, Virginia, USA 22031
voice/fax: (703) 876-0935
email: rcurts@erols.com, dcamp@aol.com

Abstract

The underlying premise of this study is the hypothesis that benefits could accrue if a more flexible and responsive methodology could be applied to how Information Assurance (IA) is mandated on the Fleet. It is the authors' contention that "information assurance" functionalities could be successfully modeled along the same lines as the "safety" functionalities performed by the Naval Aviation Safety Program. This research concentrates on a high-level review of the Naval Aviation Safety Program to determine if "lessons to be learned" could also be operationally applied to Information Assurance. The purpose was to determine those areas within the Naval Aviation Safety Program that could serve as templates or analogies to strengthen the manner in which Information Assurance is applied in the Fleet.

This continuing research follows up on the paper "Architecture: The Road to Interoperability" presented by the co-authors at the 1999 CCRP Symposium held at the Naval War College in Newport, RI [Curts & Campbell, 1999]. The recommendation offered at the end of the 1999 presentation was for an information assurance center, or IAC, that could provide monitoring and assistance and be responsible for a Fleet lexicon (a common language) and taxonomy (a common framework); standards (common interfaces); best practices (common processes and procedures); commitment (a common attitude); accountability (a common report card); and an architecture (a common blueprint). This paper follows up on the IAC concept from the Naval IA perspective

1.0 INTRODUCTION.

Just over 40 years ago, the Naval Safety Center, which includes its Aviation Safety Program, began its tenure neither liked nor respected. Many operational commanders felt that safety requirements were a "tax" on their operational goals, did not see a real value in safety inspections, and consequently did not wholeheartedly support the effort. The basic belief was that low marks on a safety inspection could have a significant, long term, negative impact on careers.

The same could be said about the various Computer Security Programs over the years. No operational commander wants to sign off on an accreditation package. The basic belief is that if

1 This study is solely a research effort. Any judgments expressed or implied are those of the authors and should not be interpreted as official Department of Defense positions. But by illuminating key Information Assurance (IA) concerns and serving as a source of information about a proposed Naval Information Assurance Center, this document serves as a valuable tool in the creation of IA policies and procedures.

something ever went wrong, like an unauthorized entry into a secure network, the responsibility would have to fall back onto the accrediting authority. Even the conduct of a friendlier vulnerability assessment to test their systems is often met with reluctant cooperation.

Today the Naval Aviation Safety Program is a completely operational program in which the key responsibilities are vested in operational units, with program support and advice from staff organizations like the Naval Safety Center (NSC) and the Safety School at the Naval Postgraduate School in Monterey, CA. The Fleet is responsible for all safety issues and has the authority and accountability that goes with such responsibility. Support organizations assist in the management of the Safety Program and provide a source of expert advice for both proactive and reactive safety issues.

The degree to which safety has been accepted by the operational units was seen as the key to this research. Roles have evolved to facilitate the safety program, and information flows regularly throughout the Navy for the purpose of increasing safety. Similarly, the criticality of information and the degree to which information assurance must be accepted by operational units has risen dramatically, yet roles have not evolved to facilitate the information assurance program.

Our research identified several recommendations where the Information Assurance community could adapt proven management techniques from the Naval Aviation Safety community.

We will conclude that there is a significant learning potential for the Information Assurance community in the analysis and emulation of the Naval Aviation Safety programs. In our research, it became clear that the Naval Aviation Safety community has clearly defined their goals, adapted a helpful attitude of providing service to their customers, and were willing to have their successes, and setbacks, held up for all to see and evaluate. As a result, the safety community has continued to receive the necessary support to manage their programs. We feel that the same success stories could be applied toward information assurance programs. Finally, we will propose the formation of a Naval Information Assurance Center in which this new approach could begin.

2.0 OVERVIEW OF THE NAVAL AVIATION SAFETY PROGRAM.

The Naval Aviation Safety Program is an operational program with key responsibilities vested in operational units, or the "Fleet," and with program support from the safety staff. The operational units are supported by the Naval Safety Center (NSC), headquartered in Norfolk, VA, and the Safety School at the Naval Postgraduate School (NPS) located in Monterey, CA.

The operational component of the program is managed by N88, the Air Warfare Division. The safety component is led by the staff of the Vice Chief of Naval Operations, as the Special Assistant for Safety Matters, N09F. This dual functionality is carried downward directly to the key department heads at the squadron level: the Squadron Operations Officer, the Maintenance Officer, and the Safety Department Head. The Squadron Operations Officer is responsible for flight operations and scheduling; the Maintenance Officer is responsible for aircraft maintenance and ground operations; and the Safety Department Head manages the Aviation Safety Program, including the Naval Air Training and Operating Procedures Standardization (NATOPS) and

ground safety programs. All three report directly to the Squadron Commanding Officer (CO), who has the ultimate responsibility for squadron operations and safety.

At the squadron level, each squadron has a dedicated safety officer who manages the squadron safety program under the direction of the squadron CO. The NSC provides support as discussed below. The Safety School provides the required education for all prospective squadron CO's and Safety Officers.

Although it is difficult to precisely state which changes caused which improvements, it is correct to state that overall safety has improved significantly as a result of the focus provided by the Safety Program. It became clear that some of the lessons learned and the techniques developed by the Safety Program could be used to strengthen the Information Assurance program, which is now being required to mature in a shorter period of time.

The Safety Program itself is a completely operational program, in which the key responsibilities are vested in operational units with program support and advice from staff organizations like the NSC and the Safety School at the Naval Postgraduate School. The fleet is responsible for all safety issues and has the authority and accountability that goes with such responsibility. The support organizations assist in the management of the Safety Program and provide a source of expert advice for both proactive and reactive safety issues.

The degree to which safety has been accepted by the operational units can be seen in the key roles that have evolved to facilitate the program, as well as in the information that flows regularly throughout the Navy to increase safety.

The "cause-and-effect" of a Naval Safety Center having an influence in reducing both the loss of aircraft and the loss of life is unknown. However, it is important to see that naval aviation mishap rate (mishaps per 100,000 flight hours) have been dropping overall since the early 1950s when angled flight decks on aircraft carriers and the Naval Safety Center came into existence. Various actions have taken place that may have directly or indirectly influenced the continuing reduction of such mishaps. These actions include:

- Angled decks on aircraft carriers
- Establishment of the NSC in 1953
- Establishment of the Naval Aviation Maintenance Program in 1959
- Initiation of the Replacement Air Group (RAG) Concept in 1959
- Initiation of the NATOPS Program in 1961
- Initiation of the Squadron Safety Program in 1978
- System Safety Designated Aircraft in 1981
- Initiation of Aircrew Coordination Training (ACT) in 1991

2.1 White-Hat Approach. It is extremely important to note that the NSC plays a "white-hat" role in all areas regarding safety. The term "white hat" is synonymous with those who provide advice and assistance in the management of the Safety Program. The NSC does not assign blame, nor are they responsible for directly ensuring safety throughout the fleet. The NSC

performs safety visits, with the safety teams spending six months a year on the road performing such visits. These are non-attribution visits in that the team comes in, audits safety, reports their findings to the Safety Officer and CO, and then "burns the notes."

Whenever the NSC participates in a mishap investigation, their only purpose is to determine the actual cause, regardless of any personnel actions proceeding in parallel by other organizations, like the Judge Advocate General's (JAG) office. To that end, the NSC has the authority to keep specific information confidential, if so requested by an individual. Over the years, this authority has been consistently upheld at the highest levels of the Navy and by the U.S. Supreme Court. Consequently, all personnel know that they can speak freely to NSC investigators and critical safety-related information can be acquired. According to those interviewed for this paper, (including personnel from the Space and Naval Warfare Systems Command (SPAWAR), the Naval Safety Center's Aviation Safety Program, and the Naval Air Systems Command (NAVAIR) Aviation Safety Team) this is one of the most critical aspects of the NSC's role and is a significant reason for their success over the years in determining the true cause of safety problems.

The importance of obtaining accurate mishap information cannot be overstated. Mishap reports, when initially submitted, may not provide a complete picture of the incident. Trained, expert investigators from the NSC help to clarify the key issues and to determine the most likely cause. As such, when the Mishap Report is completed and added to the NSC's database, it represents an extremely valuable piece of information for further study, which in the future may help predict potential problems.

Based on the degree to which the NSC has been accepted into the day-to-day activities of the fleet, as demonstrated by the following, it is evident that the NSC has successfully staved off the image of "Safety Cop" and is now truly "trusted" by the fleet.

2.2 Naval Safety Center Mission and Functions.

2.2.1 Mission. The mission of the NSC is: "...to enhance the war fighting capability of the Navy and Marine Corps by arming our Sailors, Marines and civilians with the knowledge they need to save lives and preserve resources. Of interest here is that the NSC has as its mission to "enhance the war fighting capability" using "knowledge" as its only armament. The same could be said about Information Assurance in that it is the increased knowledge that must be provided to the Information Assurance environment that will save lives and preserve resources.

2.2.2 Functions. From the NSC perspective, "knowledge" takes many shapes. The NSC assists the CNO in managing all aviation safety programs, ashore and afloat. This is accomplished by the following:

- Supporting many and varied program areas (aviation, surface ships, submarines, diving, occupational safety and health, motor vehicles, explosives and weapons, fire protection, environmental, recreational, off duty, and high risk training safety).

- Collecting and providing safety data. NSC is the repository for all collected safety data. They perform analysis on such data and respond to requests for such data.

- Participating in safety visits. NSC participates in safety surveys, safety stand-downs, maintenance malpractice, and mishap investigations. They assist the Inspector General and hold a seat on several boards and committees.

- Hazard awareness products. NSC produces and distributes the bimonthly *Approach* magazine and various safety-related newsletters; attends and participates in conferences and seminars; and publishes checklists, bulletins and messages.

2.2.3 Goals. The NSC has defined 15 goals. Exactly how they are to achieve each goal is currently under investigation by the NSC, pending availability of resources, but the conscious act of writing them down is a step in the right direction. These 15 goals are as follows:

1. Develop a sense of ownership for our mission, vision and strategic plan.
2. Improve our methods of collecting and analyzing data.
3. Standardize the quality of safety programs in the aviation, shore and afloat directorates.
4. Ensure our staff is well-trained.
5. Improve communications with our customers.
6. Increase the NSC's participation in policy-setting groups.
7. Pursue new ideas.
8. Market risk management as a part of everyday life.
9. Exploit the use of all media. Identify our target customers.
10. Better manage our resources.
11. Foster trust and openness in our relationships with our customers.
12. Establish the most effective NSC organization that best enhances our ability to anticipate and respond to customer needs and improve the safety process.
13. Have the Commander, NSC, designated Director of Naval Safety.
14. Pursue a new marketing strategy.
15. Make our customers more knowledgeable.

2.2.4 Guiding Principles. The NSC team exists to assist the naval forces (identified as their "customers"). In their dealings with these customers, the NSC is guided by the following principles:

- Be honest and cooperative and treat all customers with dignity and respect.
- Make sure our customers and their needs come first.
- Continuously improve.
- Serve as consultants and advisors, enabling our customers to recognize hazards and manage risks.

To ensure that these guiding principles are met, the NSC supports their own personnel by:

- Allowing them to exercise authority at the lowest level;
- Promoting open communications;
- Encouraging teamwork; and,
- Stimulating and supporting professional development.

2.2.5 Safety Awareness. The Safety Awareness program is the key NSC program. The Awareness program includes:

- A bimonthly safety magazine (*Approach*) directed toward the aircrews.
- Quarterly reviews by aircraft type.
- Monthly messages.
- Mishap reports to collective addresses.
- Squadron Safety Stand-down support.
- The Director of the NSC speaks to every command class (One week safety class for aviation CO's and the CO class for ships.)

2.2.6 Process Improvement. The NSC has a Process Action Team (PAT) which is reviewing the way the NSC manages the safety program. The NSC is moving toward the use of "Trip Wires" which will alert them when certain events occur. This is similar to an Indications & Warnings (I&W) Program.

2.3 Training. The key safety training is performed by the School of Aviation Safety at the Naval Postgraduate School. The mission of the School of Aviation Safety is: To educate aviation officers at all levels; to identify and eliminate hazards, to manage safety information, and to develop and administer command safety programs; to foster and conduct safety-related research; and to provide assistance in support of the Naval Aviation Safety Program; thereby enhancing combat readiness through the preservation of assets, both human and material.

2.3.1 Command Level Course. The five-day Aviation Safety Command (ASC) course is offered eight times each year at the Naval Postgraduate School in Monterey, CA. The ASC course is offered to Navy and Marine commanding officers, executive officers, officers in charge of aviation detachments, officers screened for command and staff officers in the rank of Lieutenant Commander, or Major, and above. This course is designed to provide information which will assist commanding officers in conducting an aggressive mishap prevention program and to prepare the graduate for the duties of Senior Member of a Mishap Board. The course consists of approximately 35 classroom and laboratory hours over five instructional days, addressing subjects including safety programs, safety psychology and human factors, aviation law, aircraft systems, mishap investigation techniques, mishap and incident reports and endorsements and aerospace medicine.

2.3.2 Safety Officer Course. The 28-day Aviation Safety Officer (ASO) course is offered seven times each year, on a temporary additional duty basis, for those commands needing an Aviation Safety Officer (ASO). This course prepares the graduate to assist his or her

commanding officer in conducting an aggressive mishap prevention program. When the ASO completes the course, he or she will be able to organize and administer a mishap prevention program at the squadron level as defined in OPNAVINST 3750.6 [OPNAV, 1989]. This 28 instructional-day course consists of approximately 160 classroom and laboratory hours. Subjects addressed include safety programs, risk assessment and mishap prevention techniques, operational aerodynamics and aerostructures, mishap investigation and reporting, psychology, human factors, safety law and aeromedical support. Designated naval aviators and naval flight officers of the Navy and Marine Corps in the rank of Lieutenant, (USN) and Captain, (USMC) and above are eligible to attend.

2.3.3 Additional Courses. Aviation squadron staff receive safety training at many levels. The airman is introduced to safety training in many stages as he or she prepares for the first assignment. The aviator has safety training emphasized at each stage of their training from Preflight to completion of aircraft specific training. By the time a replacement arrives in a squadron, they have a firm foundation of safety training.

2.4 Squadron CO Perspective. There are training tools and benefits present which clearly demonstrate that naval aviation safety has become ingrained in the career development/career enhancement of every naval aviator, from Airman to Admiral. The perspective can be seen at the Squadron Commanding Officer level in the formal training available to the CO and his/her staff. Every CO also has a myriad of tools available at the their disposal. Every CO understands the benefits to their squadron from the use of such tools and in participating in the safety program. The formal training has been discussed above. This training is supplemented by the squadron level programs and the NATOPS program in the squadron. There are frequent reviews and check flights for the crew member and inspections or reviews for the squadron. If any CO feels the need for additional assistance, they can request a visit from the NSC.

Squadron safety records are viewed as critical information in the evaluation of the squadron CO. A weak or poor safety record is not career enhancing. Conversely, the periodic squadron safety competition and awards are strong motivators for all members of the unit.

3.0 FINDINGS.

The purpose of this study was to determine those areas of the Naval Aviation Safety Program which ***may*** serve as templates or analogies for strengthening an Information Assurance Program. Whereas more detailed study is needed to properly determine if, in fact, the analogies hold and/or similar results will be possible, here we make some high-level observations about the Safety Program's success and draw some tentative relationships to the Information Assurance Program.

The success of the Safety Program appears to stem from the following fundamental characteristics:

- Over 40 years of evolution.
- Clear assignment of responsibility, authority and accountability to operational commanders.

- Free flow of incident and preventative information to all organizations that have a vested interest in that information.
- "White-Hat" approach to gathering information and assisting with reviews, both pro-active and reactive.
- Existence of a database of all safety-related reports, maintained by safety experts and used for a wide-range of purposes.
- Coordinated training across all ranks and specializations.

As indicated in the first bullet, success has not come quickly or easily. The Safety Program has continually evolved a role that works effectively to assist operational commanders, without usurping their authority. Whereas the information and focus lies with the Safety Center, the responsibility and authority still lies with the operational commanders. The Information Assurance programs are in their infancy, relatively speaking, and they would be well served by "developing" a similar role with operational commanders.

An Information Assurance Program that views the operational commanders as "customers" may be the only program that can hope to achieve the same level of acceptance that has been attained by the Naval Aviation Safety Program.

3.1 Visibility and Access. Without high-level visibility and access, the NSC would not be able to gather the necessary information, or provide advice to those who can make a difference. To that end, the Safety Center reports directly to the CNO. Similarly, at the squadron level, the Safety Officer reports directly to the CO.

If a similar chain of command were implemented for an Information Assurance program, the same level of visibility and access would probably result. This would provide those programs with the necessary relationships to gather and disseminate information, and to help build the level of "trust" that the Safety Program has attained. It is possible that the Information Assurance Program will never achieve the same level of trust, because it may not be possible to convince the average sailor that information assurance is a "life-threatening" issue. However, without high-level visibility and access, it is almost certain that the Information Assurance Program will not be accepted by the fleet.

How did the safety issue get elevated to its current importance? First, the Safety Program had to gain respect within the different communities. Initially, there was little visibility and the underlying thought was probably that safety was counterproductive. That is no longer true. Safety is now perceived as an important "operational" issue by the commander, because it helps preserve assets.

The increase in safety importance and acceptability came about during the mid 1970's and 1980's. The Marine Corps was first to adopt it, followed by the Navy. The Safety Officer was elevated to a Department Head level, giving him direct access to the Commanding Officer. Although not considered a "key" career-enhancing billet, it is a department head billet all the same.

Safety also became a public issue during and after the Vietnam War. The NSC kept track of, and documented, losses. From those statistics the NSC was able to recommend solutions to make things and people more safe. The NSC was able to identify the problem AND advise operational commanders how to fix the problem. After a sustained period of benefits were shown, the Safety Program was finally recognized as a valuable source for such information, and authority soon followed.

The Information Assurance Program must emulate this approach of showing positive, tangible benefits to their customers, the operational commanders. Then, slowly but surely, they will be able to make a significant impact on the overall security of the Navy and will gain the respect that is needed to ensure acceptance by the fleet.

The major difference between safety and information assurance is that safety has the visibility--they have the "smoking hole" after an aircraft accident. The "smoking hole" is a quantifiable level of destruction with possible deadly results. In the Information Assurance community, there may not even be an audit log available to prove that an unauthorized user had entered a computer system, or that there had been any intentional or unintentional corruption of data. Similarly, it is well understood that the most significant threat to most automated information systems are authorized users, not the more publicized hackers. These authorized users could glean information and disclose this information to unauthorized sources for years before they are detected.

The Information Assurance community needs to focus their attention on the severity of the problem and the potential or real losses that can occur. Once the commander is convinced that the loss or compromise of their information-intensive systems could result in the "loss" of their ship or aircraft, then the community may have achieved the desired visibility needed.

Elevating the visibility of Information Assurance within the Navy to a level comparable to that of Safety, could provide the necessary access.

3.2 Advisory Role. The NSC role is informational, not authoritative. The NSC is responsible for writing and maintaining OPNAVINST 3750.6, The Naval Aviation Safety Program [OPNAV, 1989] . The NATOPS program is a Fleet run program which is supported by the NSC. The NSC recognizes the need to standardize and has assigned a NATOPS representative for each aircraft type. However, the Fleet owns the NATOPS manual and as such they are allowed to rewrite it. The Naval Air Systems Command (NAVAIR) controls information related to the aircraft performance envelope, but the procedures (that is, the different ways to operate inside the engineering data box) can be changed by the fleet operators. These changes are coordinated on an annual basis at NATOPS conferences. All this is done with NSC working with NAVAIR and treating the fleet as the customer.

This "White-Hat" approach should definitely be given serious consideration by the Information Assurance community. For example, a Naval Information Assurance Support Team, or NIAST, (similar to "Red Teams") should be viewed by the ship or shore establishments as a group that can

help them in meeting their own responsibilities, instead of being viewed as another inspection team created to cast blame. The NIAST reports should be delivered and held in confidence in a manner similar to that of the NSC assistance visits. The Information Assurance community needs to make their expertise available without dictating solutions to operational elements. If security is truly beneficial and the Information Assurance community truly provides a net benefit, then the operational commanders will find a way to make use of their services.

Foster a role of assistance rather than of enforcement.

3.3 Accurate and Timely Information. The NSC collects and analyzes all safety data (850 different attributes), even classified data, but they sanitize and publish everything open source. They are very proactive in releasing everything they find back out into the community, with the hope that the information (e.g., what caused a "Class A" or major mishap) would assist everyone else in the Navy by preventing similar incidents from happening to them. In the Information Assurance community, it seems that incidents (e.g., insider incidents, or hackers successfully entering a network, etc.), are held in confidence and only released to a minimum number of people. Information Assurance seems to be a closed environment, and is not operating in a way that would help others prevent the same failure from happening to them. For example, threat and vulnerability information generated by the defense department is routinely labeled "No Contractor," yet we expect our integration contractors to build systems which will be resilient, resist penetration and support the Navy's needs.

The database maintained by NSC for Mishap and Hazard Reports is a critical piece of the "scientific approach" pursued by the Safety Program. Mishap Reports represent the final word on "what actually happened" during an incident, and form the basis for both reactive and proactive activities. On the other hand, Hazard Reports (HAZREPs) are more like: "this happened to us, watch out." In either case, all reports are disseminated widely so that everyone can benefit from the information contained therein. For example, a HAZREP could include information about different Very High Frequency Omnidirectional Range (VOR) sites in Europe.
This open approach is taken because, more likely than not, the information contained in one report will trigger a proactive response by someone in the fleet. Whereas the experts at the NSC analyze information for a wide-range of reasons, individuals throughout the fleet are attuned to their unique situation and needs. Sometimes, a problem reported in one area can spark the concern of one of these front-line individuals, who may then be able to avert a potential problem. Here again, it is extremely difficult to prove that a given piece of information prevented a future problem, but the continuous improvement in safety speaks for itself.

This aspect of the Safety Program is perhaps the most controversial with regard to information assurance. Historically, security information was "held close to the chest" because many felt that it would lead to increased exploitation. In recent years, security experts have reached the conclusion that if the incident information were more widely disseminated, then fewer exploitations would occur, because many problems are the result of previously known vulnerabilities. This debate will continue for some time in the information assurance community, but someone needs to start forming appropriate information flows now in order to gain benefit

from that information in the future. In many respects, it is easier to lock down the information flows later, if the data contained therein is too sensitive, then to create the information flows in the first place.

Regardless of who actually sees what information, it is extremely important to note the mechanisms used by the Safety Program to disseminate information, which is based primarily upon the type of equipment being used and the mission of a given squadron. By substituting "computer type" for "airframe type," and "system administrator" for "maintenance officer," it is clear that the operational chain of command for computer systems is roughly equivalent to that for aviation equipment. To that end, it seems plausible to disseminate security information along those lines, in the same way safety information is disseminated.

Availability of accurate and timely information assurance reports could help the Navy fleet-support-contractor team in achievement of Navy goals.

3.4 Non-Attribution Analysis. The Mishap Board is officially non-attribution because the interest lies in what needs to be done so that this mishap would not happen again, no matter who was at fault. The information gathering process, as well as the reports themselves, represent a scientific approach, which gives everyone more respect for the process. The same could be considered for "Lessons Learned" after a virus attack.

It is important to remember that accurate safety information is gathered only because of the respect afforded the NSC because of their "White-Hat" approach; determining the actual cause of the incident is their only goal. If the Information Assurance community can develop the same focus, they should also be able to develop an accurate, and therefore valuable, database of security information against which scientific approaches can be used to increase overall security.

There are three different categories of mishaps based on non-subjective factors of dollars or personnel injury. Hazard Reports (HAZREPS) on the other hand, are more subjective and include such things as "close calls." There are also non hazard reports that are written and collected and submitted. These document deficiencies, such as lost tools, in the form of Loss Tool Reports, Equipment Improvement Reports, etc. and are usually written up by logistics or maintenance personnel. If need be, and if resources are available, one could collect all these reports to research new procedures or trends, study the reliability of tools, the provider of tools, etc.

NSC is also involved in operational risk management. From an Information Assurance standpoint, we could collect data points on all the reports coming in, and suggest the best answer to reduce or eliminate future mishaps like a successful penetration of a secure site. Suggestions may range from upgrading the hardware to providing the most cost-effective software protection to procedural training.

Conduct rigorous, non-attribution analysis of significant incidents and provide responsive feedback to the fleet.

4.0 RECOMMENDATIONS.

The premise of this study was the hypothesis of similarities between management of the Navy's Naval Aviation Safety and NATOPS programs, and the Information Assurance programs. During the course of the study we interviewed experts from the Naval Aviation Safety and NATOPS communities and reviewed documentation describing those programs. In addition to the general management approach we were searching for procedures related to management goal setting, measurement of progress, and the use of metrics.

The study discovered a number of areas where the Naval Aviation Safety and NATOPS communities differ from the Information Assurance community. In particular, the Safety and NATOPS programs have complemented each other to have a significant impact on the Naval Aviation management, operational and procedures. The result has been a sharp reduction in aviation incidents since the start of these programs. These communities are continuing to look for ways to get to the next level with their PAT and Risk Management processes.

The following recommendations are provided to assist in the identification of specific actions which could be successfully "ported" to the Information Assurance community. Each recommendation may require some additional research and analysis to determine the best way to adapt those features for the Information Assurance community.

4.1 Recommendations.

4.1.1 Goals. **Develop goals for the Information Assurance program similar to those of the NSC.** Examine the NSC 15 goals and adapt their strategies and their desired outcomes to correspond with what the Information Assurance community goals and strategies.

4.1.2 Visibility and Access. Elevate the visibility of Information Assurance within the Navy to a level comparable to that of Safety. If the Information Assurance Program is to attain the same degree of success as the Safety Program, then the IA programs must have the same visibility and access. However, such a high-level position can only be effective if the operational commanders truly accept the responsibility for implementing "their own" IA programs, with the assistance of an IA Program support organization. With this elevation in visibility, an awards programs should be considered. Awards help to increase the visibility of any initiative among the rank and file. Like a Safety Award competition, an IA Award competition could be implemented.

4.1.3 Strength Through Knowledge.

- **Collect and analyze metrics on Navy IA incidents.**
- **Develop a collection and reporting structure similar to that of the safety community.**

- **Provide prompt feedback to all units with equipment similar to that involved in the incident.**
- **Invest in an effective Public Relations campaign.**

The perspective of using "knowledge" to increase the war fighting capability of the Navy and Marine Corps could be assumed by the Information Warfare community. Some Information Assurance community members could concentrate on collecting and being the repository for all collected IA data.

Of primary interest is the collection of accurate security incident reports, similar to the Mishap and Hazard Reports used in the Safety Program. A formal report should be generated once a given loss threshold is exceeded and an informal report that can be generated by anyone who wants to report something "unusual" or potentially dangerous. The current incident reporting program should be examined to determine if it is effective and could support a structure similar to that of safety incident reporting.

The information gathered could also include security metrics and would include data collected from network monitoring devices, firewalls, routers, system operators, systems administrators, AIS security officers, etc. Such information would be invaluable, not only for security purposes, but to assist commanding officers in the management of their own resources. Commanding Officers could determine for themselves how much effort is "typical" for their peers and could act accordingly, without the fear of being "ranked" against some metric defined by a support organization. In short, the information database should contain whatever the operational commanders think is necessary for them to conduct their own security programs.

NSC is on the Internet's World Wide Web (WWW) as part of its Public Affairs efforts. A search of WWW has found many Information Assurance documents placed there by academia, government and the public. There should be no reason to hide the efforts of the Navy's Information Assurance efforts. Rather, the Navy should become proactive in getting the word out as to what they do and what they plan to do. An Information Assurance community could:

- produce and distribute various IA items of interest, from posters warning the sailor not to bring in their own floppy disk without having it first checked for viruses, to more formal newsletters;
- attend and participate in conferences and seminars; and
- publish checklists, bulletins and messages.

A responsibility of a Public Affairs Office is to track and report on the history of the command it serves. Events that were meant to reduce AIS attacks should be tracked by the Navy for at least historical purposes. The history of the NSC goes back nearly 50 years; the Navy's role in IA goes back only a few short years and has the opportunity to put a Public Affairs Office in place for IA.

4.1.4 Provide Expert Advice.

- **Establish a functional equivalent to the NSC for Information Assurance.**

- **Adopt a similar role for the center, providing assistance to support the fleet war fighting capability.**

Given a central focus for such information, similar to the Safety Center building in Norfolk, VA, a cadre of technical and system management experts could be brought together to assist in the analysis and dissemination of the security information to those fleet elements to which it applies. This Naval Information Assurance Center should be provided the support necessary to ensure that Information Assurance becomes a well-established functional responsibility within each unit where it is located.

The NSC uses statistics to measure and verify trends. They are currently evaluating the use of trends to provide "trip wires" to warn of impending problems. The most common metric used at the NSC is the number of Class A mishaps (loss of aircraft/loss of life) per 100,000 flight hours. The NSC's statistical database contains 850 attributes drawn from all the reportable data required in OPNAVINST 3750.5. From that, trends and statistically significant events can be tracked and reported. Similar analysis could be possible for security-related information. The Naval Safety Center collects data on some 850 attributes, whereas only small amounts of metrics/statistics are collected by various information assurance communities. The majority of these statistics are on virus hits, virus types, etc. There is a need to capture relevant statistics on the performance of computer systems throughout the Navy, at all classified levels. Network monitoring tools may be used to capture pertinent data (e.g., before and after firewalls are put in place). What is important is not only the collection of such statistics but the storage of same so that historical trends can be measured as additional statistics are collected. Also, neither DISA nor NAVCIRT can assist anyone with the actual software patch code to fix their problems. Not only should the Navy consider participating in evaluating such incidents, but should consider being the acquisition agent for supplying the corrected code to their users.

The Information Assurance community could also develop the elements of a full-blown "Red Team", or sub-group, that would operate on both a formal and ad hoc basis and participate in IA Fleet Exercises (as the aggressor), IA stand-downs (e.g., a polymorphic virus hits a Navy computer network and immediate action is required), IA malpractice (when network monitoring shows events occurring outside the normal operating parameters), and IA investigations (system crashes, etc.).

4.1.5 Recognize Success. Establish an award system similar to the Navy Aviation Safety Awards. A key tenant of naval operations is the recognition of the squadrons and commanders who are successful beyond the norm. The "E" for Excellence is awarded for operational excellence in many areas. ???? Commanders and staff recognize the importance safety plays in this award. Separate awards are also given for safety. Information Assurance excellence could be recognized as a significant portion of one of the existing awards, or a separate award or trophy could be given to outstanding units.

4.1.6 Coordinated Training. **Redouble the efforts in bringing everyone involved in Naval automated information systems (system administrators, CSSOs, etc.) up-to-speed on their role in Information Assurance.** Security, like safety, depends upon the actions of every man

and woman in the Navy. Accordingly, the IA community could develop a training program similar to that evolved by the Safety Program. There are some 2,000 specially-trained Safety Officers in the Fleet today. Although the number of networks, system administrators or AISSOs supporting the Information Warfare community is unknown, the number is probably considerably higher. Consequently, it is probably impractical to train all of them to the same level of expertise given a Safety Officer, but it may be possible to train an equivalent number of IA Officers who could serve as the ombudsmen for security throughout the fleet. There are significant costs associated with training, but the aviation community has come to accept this as a part of the cost of doing business. The proper training of system administrators, etc., should be addressed the same way.

Currently, no centralized training, similar to the Safety School, exists for the field of Information Assurance. If such courses do exist, they are scattered about in various training curricula, and are neither standardized nor evaluated by independent third party Information Assurance professionals. There is no formal Navy training for system operators (sysops) or system administrators, and very little training for Automated Information System Security Officers (AISSOs) in the area of Information Assurance.

Proper safety training ensures that aviation commands have people who are trained and ready to respond to a mishap. They are trained to ensure that the mishap is properly investigated (i.e., that evidence is collected and preserved, etc.). A properly trained Aviation Safety Officer has a good chance of getting to the bottom line--what caused the mishap. On the Information Assurance side of the house, the CSSO should be trained well enough to work in the area of Information Assurance. The CSSO, acting as an Information Assurance professional, should be trained well enough to initiate immediate action procedures in case of natural disaster, hacker attack, etc. Nowhere in the Navy is this type of training offered.

The IA community needs to identify all of the IA training currently being provided by the Navy, and to ascertain if the sysops, system administrators and CSSO/AISSOs are being properly trained to handle their roles in IA. In the Air Force On-Line Survey study [1995 Vulnerability Assessment of Air Force Networked Computer Systems] published in May 1996, the following findings were discovered in the area of security education, training and awareness:

- System administrators indicated a limited awareness of security. Assessment teams concluded that the training received was insufficient, incomplete or ineffective.

- Only 52% of the system administrators had received any kind of security training.

- The majority perception from the system administrators (93%) is that their users are aware of their security responsibilities; results discovered in the field disputed this perception.

It should be of considerable interest to the IA community if the above Air Force Vulnerability Assessment could be repeated using Navy assets and resources to ascertain if such vulnerabilities exist within the DoN community.

4.1.7 Risk Management Program. **Develop an effective Risk Management program for Navy Information Assurance which will consider the impact of local risk management decisions on the Navy-wide infrastructure.** The Naval Aviation Safety community, as well as the Nuclear Regulatory Commission, the National Institute for Occupational Safety and Health, the aerospace industry, and many civilian companies have embraced a concept called risk management to improve their success in dealing with risk. Draft OPNAVINST 3500, "Operational Risk Management" establishes safety Operational Risk Management as integral in naval operations, training and planning, at all levels, to optimize operational capability and readiness. The Operational Risk Management process is a decision-making tool used by people at all levels to increase operational effectiveness by anticipating hazards and reducing the potential for loss, thereby increasing the probability of a successful mission. (Note, this draft instruction does not currently address security risk management.)

One concern about the use of Operational Risk Management within the Information Assurance arena is the inherently subjective nature of risk management. Prudence, experience, judgment, intuition and situational awareness are all part of an effective risk management program. Without a long-term commitment and proper foundation in IA, there can be no one capable of determining or managing such risk. One would tend to believe that an Information Assurance Officer would need to become a subspecialty designator and the Information Assurance Specialist an enlisted rating within the Navy.

However, any Information Assurance program should still consider implementing some form of an Operational Risk Management technique. It must be understood that no automated information network can be 100 percent "hacker-free." There is risk within IA and it does need to be managed. There must be some realistic goal and this goal must be addressed by all concerned. We can not encrypt everything, and we must believe in the trustworthiness of our systems.

There must be a balance between the role that information assurance measures play and the availability of the network to legitimate users. Much like the different levels of security put into place at an airport, based on the actual or perceived threats to the airport resources (e.g., airport, aircraft, the flying public), IA must be capable of operating within minimum and maximum levels of risks. An example of this risk envelope could be the operating levels set on a firewall. During periods of perceived low-risk, anyone should be allowed to attach files to an e-mail and send it out via the network. As risks increase, there should be a smaller number of users allowed to perform this function. As risks further increase, the byte size of the outgoing files could be kept to a certain level. As risks further increase, you could stop all attachments to e-mail. Risks increase when the number of packets hitting the firewall from the outside increase beyond an acceptable level. Proper training of sysops, system administrators and AISSOs would give them the knowledge needed to set the acceptable levels. Proper training using the operational risk management process would increase their ability to make informed decisions by providing the best baseline of knowledge and experience available.

It has been said that the amount of risk we will take in war is much greater than that we should be willing to take in peace. Applying the Operational Risk Management process has reduced

mishaps, lowered costs and provided for more efficient use of resources. Further research into some form of Operational Risk Management within IA is warranted. It may be feasible to look at combining the Risk Assessment methodologies used in the Naval computer security regulation OPNAVINST 5239 with that of OPNAVINST 3500.

4.2 Conclusions. The authors have concluded that there is significant learning potential for the Information Assurance community in the analysis of the Naval Aviation Safety and NATOPS programs. The recommendations above identified specific areas where additional study is merited. It was clear to us that the Naval Aviation Safety and NATOPS communities have clearly defined their goals, adapted a helpful attitude of providing service to their customers, and were willing to have their success, and setbacks, held up for all to see and evaluate. As a result, the safety community has continued to receive the necessary support to manage their programs.

Our study suggests that there is a real role for a Naval Information Assurance Center (NIAC).

We are aware that the Department of Defense (DoD) already sponsors 13 Information Analysis Centers (IAC) and the Information Assurance Technology Analysis Center (IATAC). We do not propose duplicating the functions of these centers. Our idea is that the Navy should have a "one stop shopping center" that would cover a wide range of IA activities including providing outsourcing guidance to industry. We looked at many examples and determined that the following general guidelines are pertinent for this organization:

- Established at a high level within the Navy. There should be subordinate "shadow" organizations within each department.
- Function as a "honest broker/"trusted agent" for all customer organizations.
- Be informative. It should collect and maintain a data/knowledge warehouse. This includes compiling statistics, analyzing trends and publishing this information.
- Provide for training in IA concepts, policies, guidelines and operational procedures. Ensure that IA training materials are available and provided to users.
- Ensure that a variety of IA awareness materials (e.g. posters, magazines, pamphlets, etc.) are designed and published on a regular basis.
- Establish and control an IA certification process.
- Provide guidance to include operational processes, procedures, checklists, etc.
- Provide "pre-inspection survey" support to customers as needed/requested (i.e. help identify and rectify deficiencies before formal inspection process).
- Consist of a permanent core team of Naval civilian and military personnel. This would include procurement and legal personnel with experience in contracting with industry. As required, the NIAC would be augmented with industry contractor support to provide a standing and readily available pool of subject matter experts.
- Manage the outsourcing of IA functions to industry in accordance with approved rules, regulations and procedures.
- Identify problem areas and work with customers and other organizations to develop and implement corrective actions.

The Navy should adopt an organizational concept based on the business practices formed by the Naval Safety Center and its Naval Aviation Safety Program and similar to the Information Assurance Center (IAC) depicted in Figure 1.

5.0 The National Defense Industrial Association (NDIA) IAC Concept – A Closing Note

Early in 1998, the authors participated in another study conducted by the National Defense Industrial Association (NDIA) to investigate information assurance (IA) issues on behalf of the OASD(C3I) [NDIA, 1999]. The study has not yet been released, but the basic IAC concepts put forth in this study were developed by the authors of this paper. Figure 1 was taken from that study. Though developed as a potential solution to the IA problem, the study concluded that we would not be able to solve the IA problem without first solving the interoperability issue.

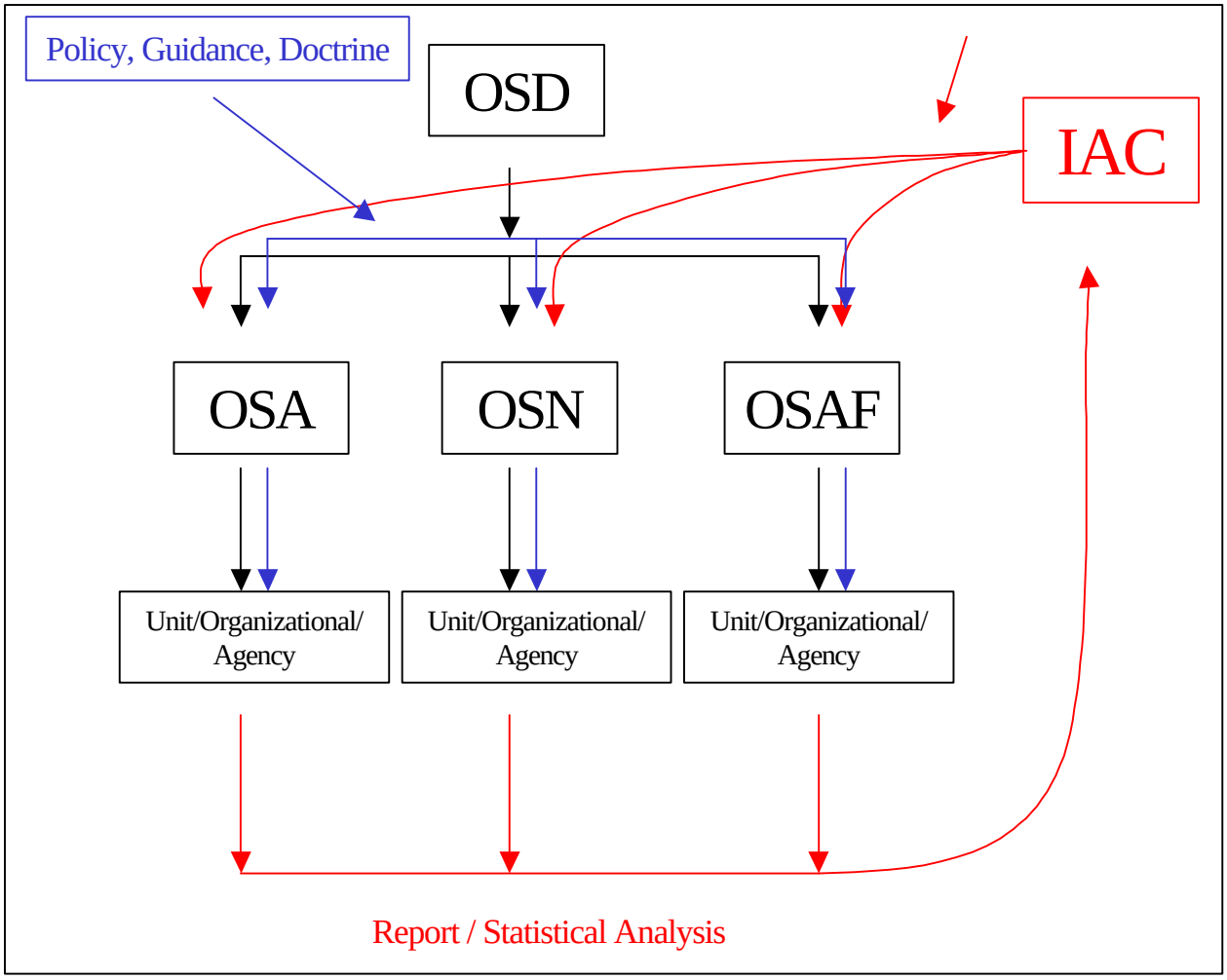

Figure 1. Information Assurance Center (IAC) Concept.

There was a good deal of concern in the IA study group about the ability of operational commanders to get the help they needed without highlighting their command's deficiencies up through their chain-of-command and, thus, potentially jeopardizing their careers. This concern mirrored the concerns found by the Naval Aviation Safety program. An information security analogy to that paradigm was presented to SPAWAR in 1997 by Dr. Campbell. It was subsequently updated and elaborated upon in the NDIA study and in this paper.

The idea is to set up an independent, high level, informative agency modeled after the Safety Center paradigm to assist, monitor and track IA issues.

5.1 Organizational Processes.

5.1.1 Introduction/Current Processes. The NDIA study began with an extensive literature search, a plethora of interviews and seminars attended by numerous industry experts in the areas of information warfare, C4ISR, INFOSEC, information defense and related fields. Early in this effort it became evident that no repeatable, accepted, organized processes, procedures, infrastructure exists within DoD, nor any of its components, to address the issues associated with IA. Current policies, processes and procedures related to Information Assurance (IA) are formulated by numerous commands at various levels within the DoD infrastructure.

Additionally, many such constructs are applicable only to one command, system, agency or some other relatively small segment of the information infrastructure. Though high level policies and procedures do exist within DoD, a recent GAO report [GAO, 1998] concluded that many decision makers are not even aware of their existence. Clearly, a better model is required. This absence of a central organizational structure and institutionalized processes was considered a major deficiency. Consequently, the study group set about to define just what such an organization might look like.

In the Fall and Winter of 1996, a study was conducted for SPAWAR to "…examine the procedures and metrics in managing the Naval Aviation Safety, Naval Air Training and Operating Procedures Standards (NATOPS), and the Navy Reliability and Maintainability (R&M) programs to then determine their crossover or relevant applicability to the Navy's Information Systems Security (INFOSEC) and Information Warfare – Defense (IWD) programs." [Campbell, 1997] The report concluded that these existing programs had direct transferability to the information security problem and that a "Security Program that views the operational commanders as 'customers' is the only program that can hope to achieve the same level of acceptance that has been attained by the Safety program."

That study (summarized above) and its authors were consulted by this study group as a basis upon which to build the overall Information Assurance Center (IAC) concept described below.

5.2 The Information Assurance Center (IAC).

The concept of an Information Assurance Center (IAC) closely follows and was, in fact, patterned after that of the Naval Safety Center (NSC). Although the roles, responsibilities and missions of such an organization remain to be solidified, there are a few general guidelines with direct similarities to NSC. Among its many functions and areas of responsibility, the IAC should:

- Be established at the highest levels of DoD possibly with components or shadow organizations within each military department. (See Figures 1&2)
- Be informational, not authoritative.
- Be responsible for writing and maintaining the Information Assurance program "Bible."
- Function as an "honest broker" / "trusted agent" with respect to "customer" commands.
- Collect and maintain a data / knowledge warehouse.
  - Compile statistics
  - Analyze and publish statistical trends
- Provide training in IA concepts, policies, guidelines and operational procedures.
- Produce and provide IA training materials.
- Design, edit and publish a variety of IA awareness materials (e.g. posters, magazines, pamphlets, etc.)
- Establish and control an IA certification process for operators, trainers, systems, programs, etc.

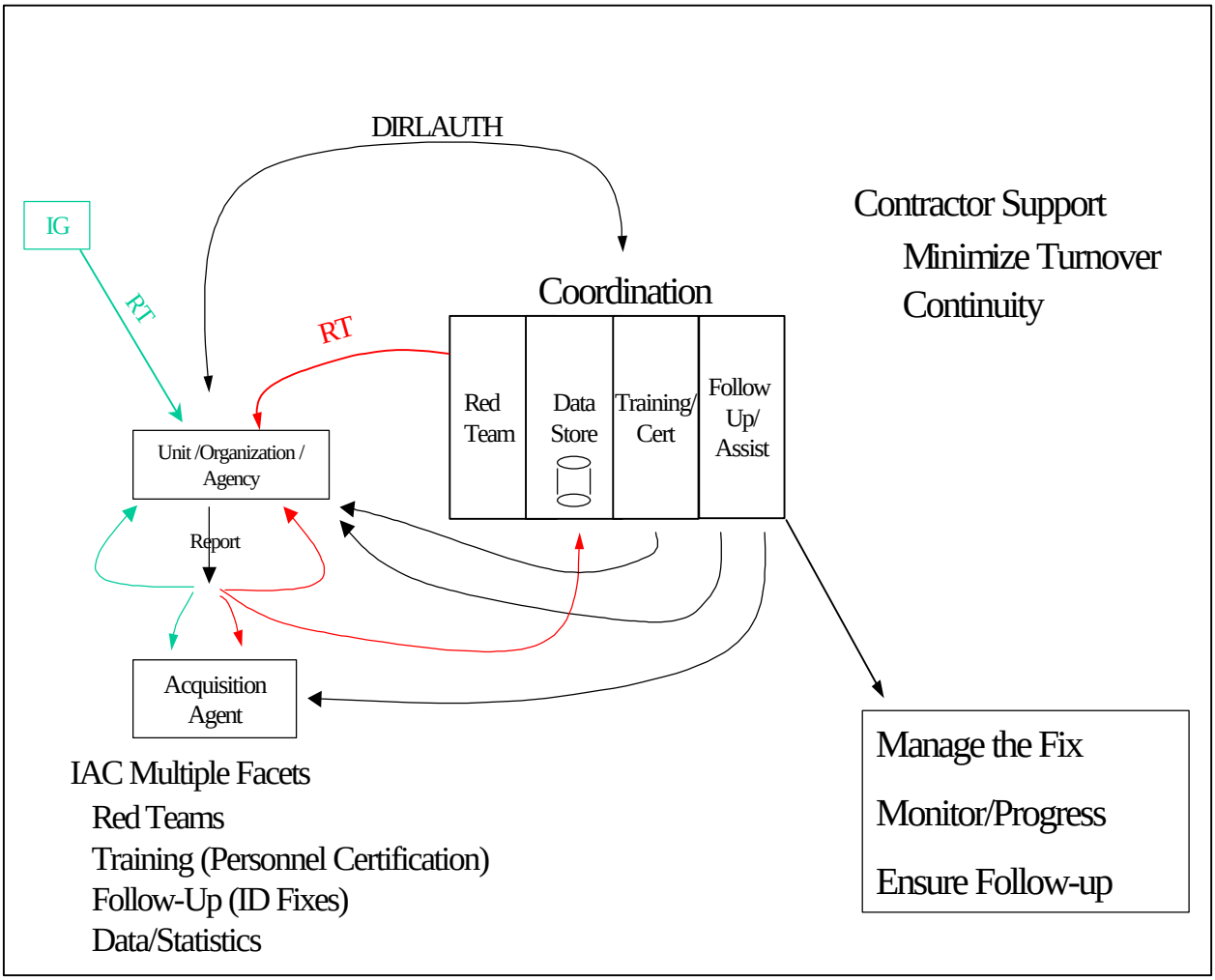

Figure 2. IAC Organization.

- Study, establish, maintain, perfect and provide operational processes, procedures, checklist, etc.
- Provide "pre-inspection survey" assistance to customers as needed / requested (i.e. help identify and rectify deficiencies before the formal inspection process and before they become a problem.) See Figure 3.
- Consist of a core group of military/DoD civilian personnel augmented as necessary with contractor support to provide a standing, readily available pool of subject matter experts (SMEs).
- Identify potential problem areas and work with operators and acquisition agents to develop and implement solutions.
- Investigate IA incidents and responses, and maintain statistical data.
- Collect information on best (common) practices within the areas associated with IA.
- Centralize, coordinate, and facilitate outsourcing IA functions to industrial partners through omnibus contract vehicles and maintaining lists of qualified companies and personnel.

Although the details of these and other functional areas remain to be worked out, there is little doubt that the concept can provide a missing dimension to the IA infrastructure that, as proven by the NSC, can result in substantial benefits.

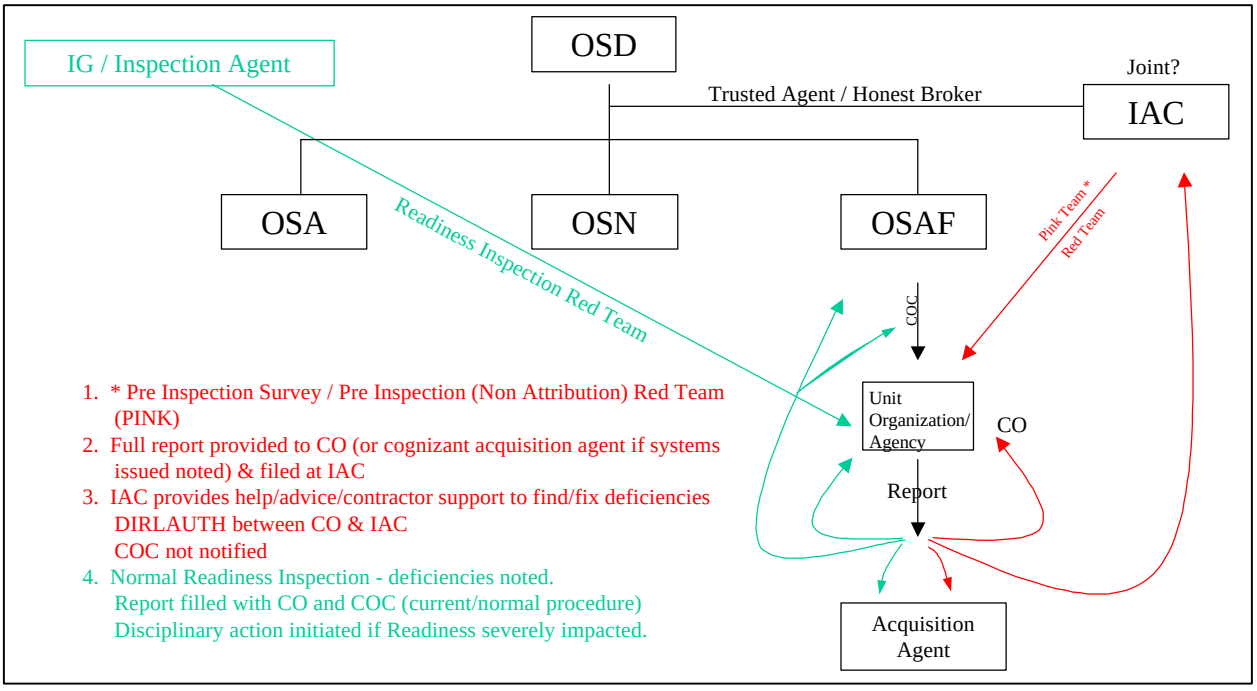

Figure 3. IAC Process.

A high level, centralized IA organization, patterned after the highly successful Naval Aviation Safety Center's Aviation Safety program could provide significant benefits to operational units and the IA community at large.

ACRONYMS AND ABBREVIATIONS

ACT	Aircrew Coordination Training
ASO	Aviation Safety Officer
CCRP	Command and Control Research Program
CCRT	Command and Control Research and Technology Conference
CNO	Chief of Naval Operations
CO	Commanding Officer
COTS	Commercial-Off-The-Shelf
CSSO	Computer Systems Security Officer
DISA	Defense Information Security Agency
DODDir	Department of Defense Directive
EIC	Equipment Identification Code
FIWC	Fleet Information Warfare Center
HAZREP	Hazard Report
IA	Information Assurance
IAC	Information Assurance Center
INFOSEC	Information Security
ISEA	In Service Engineering Activities
MTBF	Mean-Time-Between-Failure
NATOPS	Naval Air Training and Operating Procedures Standardization
NAVAIR	Naval Air Systems Command
NAVCIRT	Naval Computer Incident Response Team
NAVICP	Navy Inventory Control Point
NAVOSH	Naval Occupational Safety and Health
NIAC	Naval Information Assurance Center
NPS	Naval Postgraduate School
NSC	Naval Safety Center
PAT	Process Action Team
PM	Program Manager
PMA	Program Management Office
QA	Quality Assurance
R&M	Reliability and Maintainability
RMA	Reliability, Maintainability, Availability
RAG	Replacement Air Group
SPAWAR	Space and Naval Warfare Systems Command
VHF	Very High Frequency
VOR	VHF Omnidirectional Range
WWW	World Wide Web

References

[Campbell, 1997] Campbell, Douglas E.; Stauffer, Barry; Pittelli, Frank. "Refining the Management of IW-D Plans, Goals, Milestones and Metrics Based on Three Successful Navy Programs." Washington, DC: Space and Naval Warfare Systems Command, 20 January 1997.

[Curts & Campbell, 1999] Curts, Raymond J.; Campbell, Douglas E. "Architecture: The Road to Interoperability." Presented at the 1999 Command & Control Research and Technology Conference, U.S. Naval War College, Newport, RI.

[NDIA, 1999] National Defense Industrial Association (NDIA) Information Assurance (IA) Study Final Report (Draft, Pending Release), NDIA C4I Committee Study Group, Fairfax, VA, August 1999.

[GAO, 1998] General Accounting Office (GAO) Report on Joint Military Operations: "Weaknesses in DoD's Process for Certifying C4I Systems' Interoperability (GAO/NSIAD-98-73)." GAO: Washington, DC, 13 March 1998.

[OPNAV, 1976] OPNAV Instruction 3750.16B. Participation in a Military or Civil Aircraft Accident Investigation, 26 April 1976.

[OPNAV, 1989] OPNAV Instruction 3750.6Q. Naval Aviation Safety Program, 28 August 1989.

[OPNAV, 1997] OPNAV Instruction 3710.7R. NATOPS General Flight and Operating Instructions, 15 January 1997.

[OPNAV, 1998] OPNAV Instruction 4790.2G. The Naval Aviation Maintenance Program (NAMP), 1 February 1998.

Vita

CDR Raymond J. Curts, Ph.D., (USN, Ret.) was born December 2, 1946 in Philadelphia, Pennsylvania and is an American citizen. He graduated from Vandalia Community High School, Vandalia, Illinois in 1965. He received his Bachelor of Science in Aeronautical and Astronautical Engineering from the University of Illinois in 1970 and was commissioned as an Ensign in the United States Navy. In December 1972 he earned his wings as a Naval Aviator and was assigned to the U.S. Naval Base at Guantanamo Bay, Cuba. Returning to the continental United States in 1976, he became an instructor pilot in the Navy's Advanced Jet Training Command in Beeville, Texas where he earned a Master of Arts degree in Management and Business Administration from Webster College of St. Louis, Missouri. After tours of duty in Norfolk, Virginia; Rota, Spain; and Key West, Florida, he was stationed at the Space and Naval Warfare Systems Command (SPAWAR) in Washington, DC where he spent five years as the Navy's Electronic Warfare Architect. During this time he earned a Ph.D. in Information Technology from George Mason University.

LCDR Douglas E. Campbell, Ph.D., (USNR-R, Ret.) was born on May 9, 1954 in Portsmouth, Virginia, and is an American citizen. He graduated from Kenitra American High School, Kenitra, Morocco, in 1972. He received his Bachelor of Science degree in Journalism from the University of Kansas in 1976 and was immediately commissioned as an Ensign in the United States Navy. He joined the U.S. Naval Reserve Program as an Intelligence Officer in 1980 and was transferred to the Retired Reserves as a Lieutenant Commander on 1 June 1999. Dr. Campbell received his Master of Science degree from the University of Southern California in Computer Systems Management in 1986 and his Doctor of Philosophy degree in Computer Security from Southwest University in New Orleans, Louisiana, in 1990. Dr. Campbell is president and CEO of Syneca Research Group, Inc., a certified 8(a) company under the U.S. Small Business Administration’s program.