AD-A042 959 DEFENSE SYSTEMS MANAGEMENT COLL FORT BELVOIR VA F/G 5/1
NATO STANDARDIZATION VERSUS U.S. DATA RELEASABILITY: AN APPROAC--ETC(U)
MAY 77 G R WINTERS

UNCLASSIFIED NL

| OF |
AD A042959

END
DATE FILMED
9-77
DDC

DEFENSE SYSTEMS MANAGEMENT COLLEGE

PROGRAM MANAGEMENT COURSE

INDIVIDUAL STUDY PROGRAM

NATO STANDARDIZATION
VERSUS U.S. DATA RELEASABILITY:
AN APPROACH TO RESOLVING THE CONFLICT

STUDY PROJECT REPORT
PMC 77-1

GEORGE R. WINTERS
MAJOR USAF

FORT BELVOIR, VIRGINIA 22060

NATO STANDARDIZATION
VERSUS U.S. DATA RELEASABILITY:
AN APPROACH TO RESOLVING THE CONFLICT

Individual Study Program

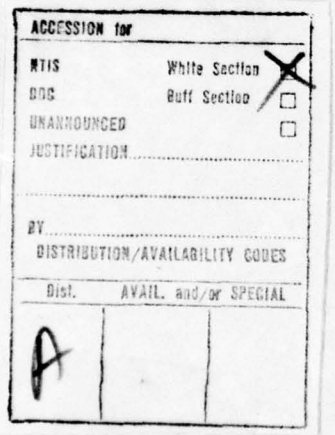
Study Project Report

Prepared as a Formal Report

Defense Systems Management College

Program Management Course

Class 77-1



by

George R. Winters II
Major USAF

May 1977

Study Project Advisor
Major Richard D. Clark, USAF

SECURITY CLASSIFICATION OF THIS PAGE *(When Data Entered)*

REPORT DOCUMENTATION PAGE		READ INSTRUCTIONS BEFORE COMPLETING FORM
1. REPORT NUMBER	2. GOVT ACCESSION NO.	3. RECIPIENT'S CATALOG NUMBER
4. TITLE *(and Subtitle)* NATO STANDARIZATION VERSUS U.S. DATA RELEASABILITY: AN APPROACH TO RESOLVING THE CONFLICT		5. TYPE OF REPORT & PERIOD COVERED Study Project Report 77-1
		6. PERFORMING ORG. REPORT NUMBER
7. AUTHOR(s) GEORGE R. WINTERS		8. CONTRACT OR GRANT NUMBER(s)
9. PERFORMING ORGANIZATION NAME AND ADDRESS DEFENSE SYSTEMS MANAGEMENT COLLEGE FT. BELVOIR, VA 22060		10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS
11. CONTROLLING OFFICE NAME AND ADDRESS DEFENSE SYSTEMS MANAGEMENT COLLEGE FT. BELVOIR, VA 22060		12. REPORT DATE 77-1
		13. NUMBER OF PAGES 39
14. MONITORING AGENCY NAME & ADDRESS*(if different from Controlling Office)*		15. SECURITY CLASS. *(of this report)* UNCLASSIFIED
		15a. DECLASSIFICATION/DOWNGRADING SCHEDULE

16. DISTRIBUTION STATEMENT *(of this Report)*

UNLIMITED

DISTRIBUTION STATEMENT A
Approved for public release;
Distribution Unlimited

17. DISTRIBUTION STATEMENT *(of the abstract entered in Block 20, if different from Report)*

18. SUPPLEMENTARY NOTES

19. KEY WORDS *(Continue on reverse side if necessary and identify by block number)*

SEE ATTACHED SHEET

20. ABSTRACT *(Continue on reverse side if necessary and identify by block number)*

SEE ATTACHED SHEET

DD FORM 1 JAN 73 1473 EDITION OF 1 NOV 65 IS OBSOLETE

SECURITY CLASSIFICATION OF THIS PAGE *(When Data Entered)*

DEFENSE SYSTEMS MANAGEMENT COLLEGE

STUDY TITLE:

NATO Standardization Versus U.S. Data Releasability: An Approach to Resolving the Conflict.

STUDY PROJECT GOALS: To define the conflict, at the program office level, between NATO multi-national undertakings and foreign disclosure restrictions. To provide a conceptual structure for analyzing such conflicts. To suggest an approach for resolving or avoiding such conflicts.

STUDY REPORT ABSTRACT: The report delineates two chains of direction which can conflict in the program office. One chain supports the national policy goal of increasing the effectiveness of NATO by standardizing systems to achieve interoperability. The other chain supports the national policy goal of protecting U.S. security by restricting the transfer of data and technology. These national policies can conflict in a program office if implementing NATO standardization requires release of vital U.S. data.

The study describes how to achieve both goals: NATO standardization and protection of U.S. data. How depends on the particular situation, and the particular situation depends on two factors. One factor is the type of data which are involved: threat data, U.S. system capabilities/vulnerabilities, or technology. The other factor is the potential disclosee: NATO government, NATO industry, or non-NATO buying government. These factors can be arranged into a three-by-three matrix which results in nine general data - disclosee cases.

For each general case, the report suggests possible strategies for avoiding or minimizing standardization - releasability conflicts. The mechanisms involve alternate threat models, sanitized system engineering documents, use of Data Exchange Agreements, and the like. Emphasis is placed on early planning for NATO standardization impacts on a program and on adding foreign disclosure specialists and administrative security personnel to the program management team.

SUBJECT DESCRIPTORS: NATO, Standardization, Foreign Disclosure, Releasability, Technology Transfer, Foreign Military Sales.

NAME, RANK, SERVICE	CLASS	DATE
GEORGE R. WINTERS, Maj., USAF	PMC 77-1	May 1977

EXECUTIVE SUMMARY

The January, 1977 revisions of DODD's 5000.1 and 5000.2 have definitized the national policy of pursuing NATO standardization and interoperability through weapon system acquisition. This goal can be achieved by sale of U.S. systems to NATO, purchase of NATO systems by the U.S., or multi-national development and production programs. At the same time that program managers are responding to this policy direction, however, they must also respond to national policy to protect information vital to U.S. security. This goal is achieved by compliance with various directives on information security and technology transfer.

Thus a program manager can be faced with conflicting goals. On the one hand, he has been directed to implement NATO standardization; on the other hand, he may be constrained from disclosing aspects of his program to NATO agencies. The dilemma can be avoided by thorough analysis and careful planning.

The key to minimizing potential conflicts between the policy of NATO standardization and the policy of protecting vital U.S. data is to understand that no two releasability-standardization situations are the same. However, certain general cases can be identified. The general cases are a function of two factors: what type of data are involved and to whom it might be disclosed. In situations involving NATO

standardization, the data types are threat data, U.S. system capabilities/vulnerabilities, and technology. The disclosee categories are NATO governments, NATO industry, and non-NATO buying governments. These factors can be structured as a three-by-three matrix which isolates nine general cases of the standardization-releasability conflict.

For each general case there are several strategies which can be applied to achieve NATO standardization while still protecting U.S. data. These strategies involve such mechanisms as Data Exchange Agreements, sanitized system engineering documents, use of NATO-developed threat data, and the like. Implementing any of the strategies involves the inputs of two relatively new members of the program management team: foreign disclosure specialists and administrative security personnel.

Once program office personnel have identified the general case which most closely resembles the situation they face, they can develop a strategy for resolving the standardization-releasability conflict. In all cases, the most important aspect is planning. If the possibility that NATO standardization might impact a program is recognized at the outset, then it can be accomodated. If provisions for NATO standardization are an afterthought, releasability problems are bound to result.

TABLE OF CONTENTS

SECTION I

INTRODUCTION

In late 1976, a respected periodical reported "Defense Secretary Donald H. Rumsfeld will emphasize standardization in the North Atlantic Treaty Organization ... and offer strong advice to his replacement to continue the effort (3:11)."[1] Yet, only an advertising page away from that statement, a senior Defense Department official is quoted as being "seriously concerned about certain long-term implications of engineering and manufacturing technology transfer resulting from the export and overseas production of U.S. weapon systems (3:9). The contrasting statements represent two diametrically opposed policies of the United States Government, and the organization where they finally clash is the Program Office.

Purpose of the Study Project

The purpose of this report is two-fold. The first is to document the new dilemma which confronts program managers as a result of having to balance the drive for North Atlantic Treaty Organization (NATO) standardization with the

---

[1]This notation will be used throughout the report for sources of quotations and major references. The first number corresponds to the listing of the source in the bibliography. The second number is the page in the reference.

requirements for information security and restrictions on technology transfer. The second is to suggest some ways in which the conflict can be minimized, if not eliminated.

Program management has always required diplomatic skills. A 100% safe system may be too complex for any human to operate; while a system perfect from the human factors standpoint may be unmaintainable. Similarly, the eventual user of the system usually wants it soon; while the system engineers often want more time in development to achieve ultimate performance. So the necessity to balance disparate influences, directives, and interest groups is nothing new.

What is new, however, is the challenge to comply with recent (January, 1977) direction to implement NATO standardization and interoperability through acquisition programs. The challenge results from the fact that habits, procedures, regulations, and inspection criteria which insure 100% compliance with the Department of Defense (DOD) Information Security Program and various strictures on the transfer of U.S. technology to foreign governments and contractors inhibit interchange with NATO. The conflict between the directives for NATO standardization and the directives for safeguarding information can be minimized or avoided, but to do so will require new ways of thinking, new procedures, and higher management emphasis. Just as program managers have coped with dichotomous viewpoints before, so will program managers cope with this new conflict. This report seeks

both to define the problem and to suggest possible ways to approach the situation so that program managers can strike an optimum balance between international cooperation and national information security.

Scope and Limitations

For much of the defense establishment, no conflict exists. A U.S. unit in Europe either can use munitions from a German depot or it can't. Those involved in programming and budgeting may see different dollar amounts as a result of NATO offsets, but they see no conflict. Even headquarters levels in the system acquisition process perceive no problem. Only in the program office where interfaces are controlled, designs are approved, and data are centralized does the conflict become apparent. For this reason, the scope of this report is limited to the system program office.

The scope is also limited by the fact that DOD Directives 5000.1 and 5000.2 levy a requirement for standardization and interoperability with NATO only. The report, therefore, is concerned only with programs with NATO ramifications. Programs involving only non-NATO nations present no problem at this time since the information security policies are unchallenged.

Even where NATO is concerned, the report focusses on programs where co-production or offset agreements are involved.

Straightforward Foreign Military Sales (FMS) programs involve little conflict since an end item is delivered, along with operation and support data, in a configuration which is controlled by appropriate executive and legislative branch procedures. As a result, the scope of this report is narrower than FMS as such.

Whereas the scope of the report is bounded by the scope of the conflict, several limitations result from constraints on the report itself. The most important of these limitations is that the report relies solely on unclassified sources and is therefore unclassified. Use of classified documents would do little more than permit use of greater detail in examples; no premises or conclusions would be altered.

The final limitation on the report is the consequence of two assumptions. One assumption is that the conflict must be resolved within the existing framework of foreign disclosure and technology transfer policies. The second assumption is that NATO standardization will continue to be a goal of United States foreign and defense policy. The most obvious answers to a conflict between NATO standardization and releasability of US data would be to modify the disclosure and transfer regulations or to give less support to NATO standardization. However, those solutions are well beyond the authority of a program manager and are therefore not considered.

Overview

The next section of this report will explore the parallel heirarchies of direction which result in difficulties in the program office. First it will discuss the rationale and implementation of NATO standardization and interoperability. Then it will consider the rationale and implementation of directives governing foreign disclosure and technology transfer.

With these two schools of thought as background, the study will define the conflict which can occur and some of its ramifications. While the problem is relatively new, several examples can be cited.

Once the conflict is defined, the first step toward resolving it is to formulate an approach to analyzing specific standardization-releasability conflicts. Such conflicts can be analyzed in terms of the type of data which is involved and the type of organization which requires the information. This breakdown of the problem results in a three-by-three matrix which can be used to reduce the conflict to manageable size.

Given the analytical framework, the report will discuss each data type - disclosee pair in the matrix. It will suggest ideas on how to resolve the conflict for each of these general cases. Some involve new ways of looking at interfaces. Others consider alternative sources or protection

systems for classified information such as threat data. Still more postulate altered management procedures. The suggestions are neither exhaustive nor fully tested. Perhaps, though, they will provide a basis for other, better ways for program management offices to work toward NATO standardization while providing full protection to US information and technology.

SECTION II

BACKGROUND

Why NATO Standardization

The most persuasive argument for NATO standardization is interoperability. How persuasive is best illustrated by considering the consequences of not having it. In the event of conflict between NATO and the Warsaw Pact, the following scenarios could happen without it. A U.S. Air Force fighter pilot finds his base has been closed by an attack and is diverted to a Royal Air Force (RAF) base. Without interoperability the RAF has no bombs which fit his racks or shells for his gun, and he cannot fly a combat mission. Likewise a German tank company on its way to the front pulls into a supply point to load ammunition only to find that it is a U.S. Army unit with only U.S. Army munitions. As a result the tanks roll away with an average of only two rounds apiece. Or perhaps an Italian escort vessel in the Mediterranean sails alongside a U.S. Navy oiler to receive fuel, but the American vessel's hose fittings are found to be incompatible with Italian ones. Only interoperability prevents such possibilities. It is little wonder that after a NATO visit in late 1976 two U.S. Senators declared "Interoperability and standardization of arms and equipment must be relentlessly pursued" (1:81).

If the operational advantages of NATO standardization are accepted, then other reasons add impetus to the drive for it. Foremost among these is the efficient use of scarce research and development (R&D) resources within the alliance: money, facilities, and technical talent. In his statement to Congress on the Fiscal Year (FY) 1977 Research, Development, Test, and Evaluation program, the Director of Defense Research and Engineering (DDR&E) reported "the U.S. ... should take the lead in cooperation in international research and development" (5:VIII-1). Cooperation is required because at the time of the DDR&E statement, seven NATO nations were pursuing ground radar R&D programs, seven were developing new ship classes, six were conducting R&D on avionics, five were building new helicopters and new jet fighters, and four nations had on-going tank programs (5:VIII-13). Even if competition by two or three parties were retained, resources withdrawn from redundant programs could provide solutions to other operational requirements which are otherwise unanswered for lack of R&D resources.

An equally compelling case can be made for cooperation in the production of weapon systems and components. Even with provisions for two sources for every item (to avoid being crippled by strikes or political decisions) economies of scale resulting from concentrating production would lead to significant reductions in the acquisition cost of military hardware.

Add to these savings those associated with not spending money for equipping multiple production lines and those associated with having fewer items in the supply system, and the possibilities either for buying more items or for reductions in defense spending become apparent. Another result of extending the production runs of systems and components is that the production base is more likely to exist if conflict should occur and replacements are needed.

A strong defense is of little value to a nation on the verge of economic collapse. Thus, the military strength of NATO depends on the economic strength of its members. NATO standardization can contribute to the members' economies in several ways. One way stems from production cooperation. By extending the length of production runs, employment can be stabilized. A second way results from the more efficient use of defense funds, making money available for more troops, more weapons, or other, non-defense use. A third important way is a consequence of technology transfer. If, as in the past, military systems incorporate the latest technology, the sharing which results from NATO cooperation will cross-fertilize various industries in the member countries. An official of the Office of the Assistant Secretary of Defense for International Security Affairs recognized this aspect of the F-16 co-production program when he stated "During the life of the program, the advanced technology associated with the system

will be transferred to the Europeans..." (4:6).

The United States receives an additional economic advantage from NATO standardization. Standardization today theoretically results in offset agreements so that participating countries receive work equal in value to what they buy, but offset calculations should include total defense expenditures in a given country by a particular partner. Because of the high cost of maintaining U.S. forces in NATO, such offset calculations would permit a favorable balance of weapon receipts for the U.S. This benefit is in addition to the savings inherent in standardization.

The military and economic advantages of NATO standardization have been recognized in various policies of the United States government. In 1976 the Congress passed and the President signed into law provisions for waiver of the Buy America Act in cases where NATO standardization would be enhanced. This policy of the Legislative and Executive branches has been tested and upheld in the Judicial branch. The test case involved a complaint by a U.S. manufacturer that procurement of .50 caliber machine guns for U.S. tanks from Belgium's Fabrique Nationale (FN) was unlawful. The government was vindicated, and the Army is procuring a weapon which is not only standard in other NATO forces but which is of better quality than any U.S. product.

Within the Department of Defense, several policy directives have been issued to further the drive for NATO

standardization. DODD 4120.18 details the introduction of the metric system in the U.S. military. Since the United States was the only NATO member which had not previously adopted the metric system, standardization will be enhanced by this step (2:33). Of most impact to program managers however, is the issuance of revised DODD's 5000.1 and 5000.2 in January, 1977. One of the major changes in these directives is great emphasis on NATO standardization. One paragraph in DODD 5000.1 now states "When a new development or modification is essential, the mission needs of other DOD components and NATO shall be considered including the requirement for NATO standardization and interoperability" (7.6). This policy is implemented further in the new DODD 5000.2. Specifically, at Milestone I NATO standardization and interoperability requirements must have been "adequately considered" while at Milestones II and III NATO standardization and interoperability requirements must have been "satisfied" (8:Encl.2).

Emphasis on NATO standardization is not likely to go away. Numerous Memoranda of Understanding (MOU) have already been signed with NATO nations for trade or co-production. The F-16 and FN machine gun programs which illustrate co-production or purchase among NATO nations have been mentioned. Other examples include the Franco-German Roland air defense missile which is being produced in the U.S. for the Army and the British Harrier which has been delivered to the U.S. Marine Corps. And indications are that the new administration

will continue the policy. The new Director of the State Department's Bureau of Politico-Military Affairs, writing in Foreign Policy Magazine before assuming his job, stated that conventional weapons trade with NATO was not controversial (9:A8).

Why Protect U.S.Data

The most persuasive argument for protecting U.S. data is security. How persuasive is best illustrated by considering the consequences of not having it. In the event of conflict between NATO and the Warsaw Pact, the following scenarios could happen without it. A U.S. Air Force fighter squadron, assigned to destroy a command center, carries precision guided munitions to the target. But because an agent in an Alliance factory producing the same munition has obtained its design, the Warsaw Pact can counter the guidance system and the target survives. Or perhaps a U.S. Army artillery battery is ordered into action only to be bombed and destroyed en route because the orders were intercepted on radios copied by the Soviets from a sample smuggled out of a European depot. Similarly, a U.S. Navy destroyer in the Mediterranean is sunk by a cruise missile which homes on the ship's radar emissions while jamming them. This Pact capability is the result of poor electronic warfare discipline by a similarly equipped NATO ship several years before. It is little wonder that such documents as the DOD Information Security Program

Regulation lay down stringent requirements to control and protect classified information on new or deployed weapon systems.

If the operational advantages of protecting U.S. data are accepted, then other reasons add impetus to the drive to protect them. Foremost among these is the need to protect threat data. If the U.S. understanding of the threats our forces face became widely known, the sources of our information could probably be inferred by our potential adversaries. As a result they could cut off our sources, and threat information would be denied us. Without knowledge of the threat, U.S. designers might not provide weapon systems capable of defeating enemy systems.

Another factor which supports withholding of U.S. data is industrial readiness. In the event of a conflict in Europe, U.S. forces must be certain of reliable sources of replacement weapons and parts. For this reason, all items and components must be domestically manufactured so that supplies are not cut off by military, terrorist, or political action. In order to maintain our industrial base, defense contracts must be provided to U.S. contractors.

An equally compelling case can be made for protecting U.S. technology. Even if there were no operational consequences to providing technology to other nations, the economic consequences could be dire. If, after the investment of many

dollars in research and development, the U.S. government permitted uncontrolled export of high technology, U.S. companies would find themselves competing at home and abroad against foreign manufacturers who had copied or duplicated the new technology. Prominent Britons argue that the transfers of rights to radar and jet engine developments to the U.S. during World War II are at least partly responsible for the decline of the British economy.

The U.S. has an additional economic interest in protecting its data. As long as our technology is in the forefront, other nations which desire state-of-the-art weapon systems must come to the U.S. to buy them. Such Foreign Military Sales (FMS) provide a favorable balance of trade as well as diplomatic leverage. Futhermore, by extending the production runs of U.S. systems, the capital costs of plant and equipment are spread over more units, resulting in savings to the Department of Defense. Likewise, part of the price of FMS sales can be a recoupment of R&D costs which is a further savings to DOD.

The military and economic advantages of protecting U.S. data have been recognized in various policies of the United States government. The basic classification scheme is delineated in Executive Orders, and the legality of the system has been upheld in the courts several times. Various agencies in the government have issued implementing directives to cover topics such as atomic energy, intelligence information, export

licenses, and the like. Within the Department of Defense, directives deal with two major topics: information security and foreign disclosure.

These directives impact the program manager in the same two areas. The information security directives require preparation of a Classification Guide for every system. By assessing the potential harm to the U.S. of the disclosure of particular data items, members of the program office and information security specialists determine what the classification of those items is. The guide then becomes directive, and information classified according to it is handled under the provisions of the DOD Information Security Program Regulation and service implementing procedures. Foreign disclosure decisions, on the other hand, are handled outside the program office by foreign disclosure specialists, and all requests for disclosure must be referred to them. The classification of a data item is a major factor in the decision as to whether or not it can be disclosed.

Emphasis on protecting U.S. data is not likely to go away. In spite of major controversies surrounding publication of the Pentagon Papers, the deletion of material from books by ex-CIA employees, and the leak of information from a Congressional committee investigating the CIA, there has been no call to do away with procedures for protecting information vital to the security of the United States.

SECTION III

THE PROBLEM IN THE PROGRAM OFFICE

Goal Conflict

As we have seen, the United States government has adopted two important policies. First, we are dedicated to NATO standardization. Second, we intend to protect information vital to national security. In one sense the goals of standardization and protection are complementary. To the extent that NATO forces grow more effective, U.S. national security is enhanced. And to the extent that U.S. data is well protected, the effectiveness of U.S. forces in NATO is enhanced. So both goals are laudable.

However, situations could arise in which the goals are at cross purposes. Suppose that NATO effectiveness could be enhanced by adopting throughout the Alliance a U.S. electronic warfare system to defeat Warsaw Pact anti-aircraft gun and missile systems. But also suppose that the compromise of that electronic warfare system would result in decreasing the effectiveness of the U.S. strategic nuclear deterrent. Should the objective of NATO standardization take precedence? Or should the objective of protecting vital U.S. data take precedence?

Program Office as Intersection Point

A decision of such gravity might well be made at a high level. That particular decision might be made by Cabinet members, the level which originated the two policies whose goals are in conflict. In fact, however, the key level in such a goal conflict situation is the one at which attempts to implement both policies result in the problem. For if the problem is unrecognized, or if it is mishandled or if it results in a wrong decision at that level; the consequence may be detrimental to both U.S. national security and the interests of NATO.

The intersection of the two policies does not normally occur at the Department of Defense level. The standardization policy falls within the purview of the Director of Defense Research and Engineering. The policies on information security emanate from elsewhere in the department. Likewise, the goals flow down through different functional chains in the services and in the headquarters of the various acquisition commands. The organization in which they intersect, and therefore might conflict, is the program office. For it is in the program office that DOD managers both originate weapon system data and protect it. It is the program manager who is responsible for specifying NATO-standard features, originating classification guides, evaluating NATO industry proposals,

protecting classified information on threat or capabilities, and generally integrating the myriad of elements which comprise a modern defense system. The program office is the organization which sits at the intersection point of the national policy to implement NATO standardization with the national policy to protect U.S. data in the interests of national security.

The problem is not an unlikely one. Even such mundane items as training equipment can be affected. For example, the MOU with the European Participating Governments (EPG) which are procuring F-16 aircraft stipulates that 10 per cent of the value of U.S. aircraft, 40 per cent of the value of EPG aircraft, and 15 per cent of the value of aircraft sold to third parties will be produced in the EPG economies. One technical area in which the offset work might be offered is aircrew training devices. However, as the U.S. has heretofore done business, security restrictions and technology transfer policies would prevent placing aircrew training equipment contracts with European contractors. For one thing, designing and producing a device which authentically replicates the actual F-16 would require disclosure of the fire control algorithms and other operational flight program characteristics which are the heart of the F-16's performance. Other aspects of the F-16 system would also be identified to the training equipment contractor. To properly reproduce the electronic

warfare environment for a pilot trainee requires data on both the electronic warfare devices installed in the aircraft and the capabilities and characteristics of the electronic warfare threat. The same problem arises in providing proper training for air-to-air and air-to-ground weapon delivery. Clearly, the goals of NATO standardization and protection of U.S. data are in conflict.

The program manager in this situation is faced with three choices. First, he can restrict training device competition to U.S. companies and find offsets elsewhere. Second, he can seek to release the U.S. data at the risk of damage to national security. Third, he can implement new ways of doing business so that he can solicit European contractors without releasing vital U.S. data.

Because the program office is located at the point of goal conflict, it is the site of origination of potential problems. Conversely, it is also the site of origination of potential solutions. Careful analysis of potential conflict situations and proper planning to minimize problems can result in satisfying both goals. The remainder of this paper is devoted to suggesting an approach which permits just that.

SECTION IV

MATRIX APPROACH TO ANALYZING A RELEASABILITY SITUATION

"A Rose is not a Rose"

Careful analysis of a potential standardization-releasability conflict is the most important step to minimizing problems. Both the magnitude of the problem and the range of solutions change as the situation changes. The problems posed by discussing threat information with a military officer from a NATO country are much different than the problems associated with permitting a non-NATO, buying government to have access to new, high-technology manufacturing processes. This fact is crucial to avoiding embarassment in the process of implementing NATO standardization while protecting vital U.S. data. There is no single "standardization-releasability problem;" there is no one "standardization-releasability solution."

The two major characteristics of any standardization-releasability conflict are what kind of data is involved and to whom it might be released. Each combination of these two characteristics results in a distinct situation.

Disclosee Categories

In situations which involve NATO standardization, three categories of possible foreign disclosees can be identified.

These categories are NATO government, NATO industry, and non-NATO buying government. While these categories are nearly self-explanatory, some elaboration is required.

The category "NATO government" includes defense agencies of governments which are members of the NATO military alliance. Thus Canada is included while France is not. Likewise, Britain's Royal Air Force is included while education ministries are not. This category does not differentiate between NATO allies who have signed MOU's and those who have not. It also makes no distinction as to whether a U.S. system is being adopted by NATO or whether the U.S. is adopting a NATO system.

The category "NATO industry" includes any organization, government or privately owned, located within countries which are members of the NATO military alliance that is a potential contractor. The definition implies that such companies or arsenals have or could qualify for defense contracts from their own governments. Here again the situation could be either NATO production of a U.S. system or U.S. production of a NATO system.

The category "non-NATO buying government" includes any potential customer for a NATO-standard, U.S.-designed or produced system who is not a member of the NATO military alliance. "NATO standard" in this context does not include items which have been supplied by the U.S. to NATO through direct foreign military sales. That is, if sale of a U.S.

system to a non-NATO government does not involve offset or co-production agreements with NATO allies, normal Foreign Military Sales procedures would be applied. This category does include sale by a NATO nation to a third party of a system to which the U.S. has contributed data or technology.

Data Categories

Just as there are three categories of disclosee, so are there three categories of data. These categories are threat, U.S. system capabilities and vulnerabilities, and technology. Here again the categories are nearly self-explanatory, but some elaboration is required.

"Threat" data is restricted to the threat which is common to the United States and its NATO allies. With minor exceptions, the threat data is thereby limited to the Warsaw Pact and to those forces and systems which could be used in a European/North Atlantic scenario. Strategic nuclear forces are one obvious example of the type of threat which is not included in this category.

"U.S. system capabilities and vulnerabilities" data include performance parameters, design details, and employment information. It includes those aspects of systems and equipment which would be disclosed to potential users. Nuclear delivery capabilities and tactics would be excluded under this definition. However, this category does include disclosures which might be made in the course of detailing U.S. deficiencies

or requirements to the developer of a NATO system in which the U.S. is interested.

"Technology" includes design concepts, manufacturing techniques, scientific principles, instruments, and machinery which are inherent in the development and production of a system or equipment. These data are defined to be those which have been paid for by U.S. industry or the U.S. government. The question of control over technology developed under whole or partial U.S. government funding by a NATO establishment is a particularly difficult one which is included in this category.

Data-Disclosee Matrix

Each pair of data category and disclosee category constitutes a separate case of the standardization-releasability conflict. One way to visualize the possible combinations is to construct a three-by-three matrix of the data and disclosee categories (Figure 1).

Figure 1 represents the key to handling releasability situations which arise as the result of working toward NATO standardization. Analyzing the facts of the particular situation to determine what matrix entry represents the general case will lead program office personnel to the types of strategies which might be applied in the given case. The next section will deal with each of the general cases individually.

DATA - DISCLOSEE MATRIX

DISCLOSEE / DATA	NATO GOVERNMENT	NATO INDUSTRY	NON-NATO BUYING GOVERNMENT
THREAT	Threat to NATO	Threat to Industry	Threat to Third Party
U.S. SYSTEM CAPABILITIES/ VULNERABILITIES	Capability/ Vulnerability to NATO	Capability/ Vulnerability to Industry	Capability/ Vulnerability to Third Party
TECHNOLOGY	Technology to NATO	Technology to Industry	Technology to Third Party

Figure 1

SECTION V

STRATEGIES TO RESOLVE CONFLICT

Threat Data to NATO Government

In some respects this situation is the easiest to work around. Since the U.S. and her NATO allies are concerned with a common threat where standardization is involved, several channels already exist for government-to-government threat sharing. Where a formal Data Exchange Agreement (DEA) exists, transfer of threat data may be possible without further effort. Foreign disclosure personnel have this information and serve as the conduit for exchange of threat data.

If no DEA exists or if its provisions do not pertain to the threat data of concern, one possible solution is to create or modify a DEA. This process is a time consuming one, however, and must be largely left to the foreign disclosure community. The higher the priority of the program, the more possible this strategy becomes.

A third solution to the problem of threat data releasability lies in using the NATO developed threat. If, upon examination, the NATO threat appears valid for application to the program, it can be used. Implementing this strategy requires adopting additional administrative security procedures peculiar to handling NATO-classified materials.

Guidance in this area is available from administrative security functional experts. Once the administrative procedures have been adopted, it becomes a relatively routine process to request needed data through service channels to the appropriate component commands in NATO.

U.S. System Capabilities/Vulnerabilities to NATO Government

When the United States is interested in purchase or joint development of a NATO system which originates in an Alliance government owned arsenal or factory, that case should be considered in the category of U.S. System Capabilities/Vulnerabilities to NATO Industry.

When the case involves sale of a U.S. system to NATO, difficulties evaporate once the U.S. government and a NATO government have negotiated an agreement for the sale. Those sub-systems or components which are included in the sale are disclosed freely while those which are not included in the sale are withheld.

A problem can arise prior to an agreement, however. At early stages the best strategy is to depend on open data to initiate discussions. U.S. contractors are best equipped to provide such information and are familiar with the procedures for obtaining clearances to exhibit at such trade fairs as the Paris Air Show. Considerable program office effort is often required to facilitate these demonstrations, but the releasability problem is insignificant once the decision has

been made to permit display.

At the stage of negotiations where a serious prospective customer needs information in greater depth and detail, a Data Exchange Agreement eases the difficulty. When one does not exist or is inadequate, once again the best approach is to initiate or modify one with the aid of the foreign disclosure community.

Perhaps the easiest way to minimize problems in this matrix category is to frequently and conscientiously review the program's security classification guide. As systems progress through the acquisition cycle, many categories of data require a lesser degree of protection. Administrative security specialists can be of assistance in assuring that releasability problems do not occur because of a behind-the-times classification guide.

Technology Transfer to NATO Government

Where the potential transfer of technology to a NATO government concerns a NATO government owned factory or arsenal, it should be considered in the category of Technology Transfer to NATO Industry.

With the above exclusion, this category becomes a rare one. Normally, exchanges between the U.S. government and NATO governments on weapon systems and equipment are limited to the "whats" rather than the "hows". That is, what an item can do is of legitimate interest to potential buyers; how it

does it or how to make it is seldom their concern. In those instances where such transfer is necessary it must be covered by a DEA.

Threat Data to NATO Industry

This category is best avoided. Most instances in which it appears that the threat might have to be released are the result of "business as usual" in the program office. Often the drafters of specifications and statements of work either incorporate the threat or append it. When the possibility of NATO co-production, NATO offsets, or U.S. purchase of a NATO development exists, additional effort must be extended to sanitize such system engineering documents. One approach is to make them functional; that is, expressed in terms of what outputs are necessary.

When the specification or statement of work can not be sanitized, an alternative is to break out the particular component or subsystem and withhold it for U.S. development or production. If a breakout is made, the interface must be controlled and the specification and work statement for the remainder must document the interface. Breakout is facilitated by building the work breakdown structure with potential releasability problems in mind.

The only other satisfactory procedure in this case is to have the NATO fabricator rely on threat data supplied by his national authorities. The end item must then be carefully

qualification tested by U.S. military authorities to assure that it meets U.S. or NATO requirements.

U.S. System Capabilities/Vulnerabilities to NATO Industry

This case is most likely to occur when a U.S. program office is interested in a NATO-developed system to meet its requirement. Threat aspects of discussions would be handled as above, but descriptions of deficiencies in present systems or of unfilled requirements constitute disclosure of U.S. vulnerabilities or lacks of capability. The best approach in this situation is again to couch all discussions in functional terms; that is, what we want a system to do. Requests for Proposals where a NATO response is contemplated must be sanitized in accordance with this principle.

The other likely occurrence of this case would be the use of NATO industry to modify or overhaul already deployed, U.S. developed systems. Here again the first step is to redetermine that the data being protected still requires the previous degree of protection. A second approach is viable in cases where the industry's parent nation is a user of the system. In that instance, any necessary capability/vulnerability information should be supplied by the national authorities.

Technology Transfer to NATO Industry

Most difficulties in this category are resolved by either the export licensing process or in the negotiations

leading up to an offset or co-production agreement. Where releasability problems still exist the best approaches are again to sanitize system engineering documents or to break-out and withhold the unreleasable components.

Good planning is the key to minimizing technology transfer problems. If the work breakdown structure is built with potential technology transfer problems in mind, then it will be relatively easy to control interfaces and configurations involving modules which must be developed or produced in the United States. Similarly, early planning will permit development of functional specifications and statements of work. On the other hand, trying to implement NATO offsets or co-production after the fact is likely to be both frustrating and embarassing because of delays or refusals in the technology transfer approval process.

Threat Data to Non-NATO Buying Government

This case must be covered by a DEA. Generally speaking, sales of U.S. systems outside NATO are governed so strictly that a potential customer must convince our government that he faces a threat. Under these circumstances, release of U.S. threat data with respect to the third-party buy of a NATO-standard system is probably unwarranted. If it is and a DEA does not cover the data, one must be negotiated or modified.

U.S. System Capabilities/Vulnerabilities to Non-NATO Buying Government

For the most part, this case parallels the NATO government situation. Once a sale has been agreed to, there is little if any problem. During and before negotiations, a DEA eliminates the problem. In the absence of a DEA, discussions must be based on open information. The services of foreign disclosure and administrative security specialists are invaluable in this situation.

Technology Transfer to Non-NATO Buying Government

The most likely situation in this category involves repair and overhaul procedures and equipment. Few problems should arise in the case of deployed systems, but if they do, provisions must be made to make repairs at U.S. or NATO facilities. In that case, spare levels must be adjusted to account for items in the repair pipeline. Here again, periodic review of classification guides and arranging for an applicable DEA are the easiest ways to head off difficulties.

U.S. program offices which are acquiring NATO developed systems or equipment have an additional pitfall in this category. If the U.S. has contributed any technology or components to the NATO manufacturer, the transfer must include continuing U.S. control of that technology to third parties. This special case requires assistance of foreign disclosure

personnel at the time the technology is transferred from the U.S. Waiting until transfer to a third party is imminent will be too late.

SECTION VI

CONCLUSION

Summary

The January 1977 DODD's 5000.1 and 5000.2 have directed implementation of NATO standardization through the mechanism of system acquisition. At the same time, system acquisition organizations are required to maintain strict adherence to information security and technology transfer directives. The goals of these two policies can come into conflict in the program office. As the report of a DSMC workshop of program managers phrased it, "of particular concern is ... determination of releasable items versus those which must be safeguarded" (9:8).

It is possible to minimize the difficulties which might otherwise arise by thorough analysis and careful planning. The object of this report has been to provide a framework for that analysis and to suggest a few strategies which might be used in planning. The analytical technique is based on a matrix whose entries are data type and disclosee category. Each pairing represents a general releasability situation which can be solved. Using this matrix to identify a specific releasability problem from the broad spectrum of possible problems is the key to avoiding the standardization-releasability conflict.

The key concept in dealing with any of the specific categories of situations is planning. With proper planning, there is time to arrange for Data Exchange Agreements. With proper planning, the work breakdown structure or specification can be tailored to avoid releasability problems. With proper planning, alternate sources of threat models can be explored. Without proper planning, releasability problems will occur.

Implicit in the strategies which are offered is the need to call on functional areas which may be new members of the program management team: foreign disclosure personnel and administrative security specialists. If potential problems are analyzed early and if the advice of these functional specialists is sought early, any strategy for avoiding conflict can be implemented.

Implications

In all likelihood, the drive for NATO standardization will continue. One happening which supports this contention is the fact that, four days after his inauguration, Vice President Walter Mondale departed for Europe to reassure our NATO allies of the continuing support of the United States.

As the new DOD directives are applied and as the drive for NATO standardization gathers steam, the effects of NATO standardization will be felt in nearly every program office. As more offset or co-production agreements take effect, the greater the likelihood that any U.S. program may find that it

is expected to adopt a European produced component. The closer the alliance comes to total interoperability, the greater the likelihood that any U.S. program may find that it is procuring its product for a number of NATO nations.

As more and more programs are touched by NATO standardization, the more likely it is that releasability problems will occur. The only way to avoid these difficulties, which could be detrimental to NATO standardization and interoperability, is to adjust our system acquisition procedures to account for NATO standardization. The pay-off in both dollars and combat effectiveness is too great to consider doing otherwise.

Perhaps the best word to summarize the approach to minimizing NATO standardization versus U.S. data releasability difficulties is "sensitivity". If program office personnel are sensitive to the requirement for NATO standardization and realize their way of doing business may have to be altered, then the potential for conflict is greatly reduced. If this report has in any way increased that sensitivity, its goal has been achieved.

BIBLIOGRAPHY

1. Aerospace Daily. Washington: Ziff-Davis Publishing Co., Vol. 82, No. 12, November 16, 1976.

2. Air Force Magazine. Washington: Air Force Association, March, 1977.

3. Aviation Week & Space Technology. New York: Mc-Graw-Hill, Inc., November 29. 1976.

4. Bowman, Maj. Gen. Richard C., USAF, "The Compelling Reasons for NATO Standardization," Commanders Digest, Vol.19,No.19. Washington: Dept. of Defense, September 8, 1976.

5. Currie, Malcolm R., Program of Research, Development, Test and Evaluation, FY 1977. Washington: Dept. of Defense, February 3, 1976.

6. Defense Systems Management School, Report on "Program Management Office Implementation of Foreign Military Sales" Workshop. Ft. Belvoir, VA: DSMS, 1 April 1976.

7. Department of Defense, Major System Acquisitions, DODD 5000.1, January 18, 1977..

8. _____, Major System Acquisition Process, DODD 5000.2, January 18, 1977.

9. Washington Post. Washington: Washington Post Co., March 27, 1977.