Inter-Office Memorandum

To	IFS and Grapevine administrators	Date	August 24, 1982
From	Ed Taft	Location	PARC/CSL
Subject	Access controls (2nd edition)	File	[Indigo]<IFS>AccessControls.bravo

XEROX

In recent years, the Xerox Research Internet has grown to encompass a large number of organizations, including some outside the United States. Because of this, it is no longer possible to ignore the necessity of controlling access to electronic information resources within the Internet.

In this memo, we outline the information security requirements that must be met, and then describe the procedures for achieving them by means of the IFS and Grapevine access control mechanisms.

This discussion assumes a world in which all users are registered in Grapevine and all IFSs use Grapevine for authentication and access control. This is not yet the case. Organizations that have not yet converted are strongly encouraged to do so, since fulfilling the information security requirements is difficult or impossible without the mechanisms provided by Grapevine.

While this memo focusses on information stored in files on IFSs, much of the material is of more general relevance and applies to electronic and non-electronic information of all kinds.

These policies and procedures have been developed by a committee consisting of Andrew Birrell, Jerry Elkind, Mike Schroeder, and Ed Taft.

Changes since the March 13 edition: A new category of people has been defined, *temporary visa employees and affiliates*, along with guidelines on such people's access to electronic information. The Auto registry has been created for registering Grapevine individuals which represent machines or programs.

1. Xerox information security requirements

Within Xerox, information is classified into five categories:

1. *Public-domain* information that which has been formally cleared for public release outside Xerox.
2. *Proprietary* information all information not cleared for public release but not included in one of the following more restricted categories.
3. *Private* data information whose unauthorized disclosure could have a substantial detrimental effect on the operations of the company.
4. *Registered* data information whose unauthorized disclosure could cause serious damage to the operations of the company.
5. *Personal* data information of a sensitive, personal nature.

Information in the last two categories is subject to very stringent regulations on how it may be disseminated and stored. Since relatively few people have occasion to deal with registered and personal data, we shall concentrate on the other three categories. For information on correct handling of registered or personal data, consult your manager or your Security Coordinator.

For each category, there are guidelines for how the flow of that information should be controlled. Some of these guidelines are intended to protect Xerox proprietary concerns, while others are imposed by U.S. Government regulations.

For the purpose of describing appropriate degrees of access to Xerox information, we divide the universe of people into five groups:

1. *U.S. employees and affiliates* U.S. citizens and permanent residents who are employees of Xerox organizations and subsidiaries in the U.S., and other U.S. citizens or permanent residents who have signed non-disclosure agreements with Xerox. This also includes employees of Xerox organizations in Canada.

2. *U.S. non-affiliates* U.S. citizens and permanent residents not in category 1.

3. *Foreign affiliates* foreign nationals who are employees of Xerox Corporation or Xerox foreign subsidiaries, and who are located outside the U.S.

4. *Temporary visa employees and affiliates* foreign nationals working in the U.S. under temporary visas, who are employees of Xerox Corporation or of Xerox foreign subsidiaries.

5. *Foreign non-affiliates* foreign nationals not in categories 3 and 4.

Persons in each of these groups are permitted access to categories of information on the following basis:

1. U.S. employees and affiliates:

    a. may have unrestricted access to *public-domain* and *proprietary* information;

    b. may be given access to *private* data on a need-to-know basis.

2. U.S. non-affiliates:

    a. may be given access only to *public-domain* information.

3. Foreign affiliates:

    a. may have access to *public-domain* information;

    b. may have access to *proprietary* information on a per-project basis only; project-wide approval by the International Deputy is required (see section 5.1), and information transfers *require* Export Control Coordinator approval and any other approvals that the organization owning'' the information decides are appropriate;

    c. may be given access to *private* data on a need-to-know basis; project-wide approval by the International Deputy is required, and information transfers *require* Export Control Coordinator approval (see section 5.1) and the other approval associated with private data information.

    d. A record must be kept by the Export Control Coordinator of all transfers of non-public-domain information to foreign affiliates; the procedure for this is outlined in section 3.3.

4. Temporary visa employees and affiliates:

    a. may have unrestricted access to *public-domain* information;

    b. may have access to *proprietary* information in categories authorized in writing by the employee's Xerox manager, as described below in (d);

    c. may be given access to *private* data on a need-to-know basis as authorized in writing by the employee's Xerox manager, as described below in (d);

    d. must have their access to *proprietary* and *private* data controlled and documented according to the procedure presented in section 3.4. This procedure requires that an authorization memo be written by the employee's Xerox manager when the employee starts work as part of a Xerox group, stating the term of employment, the program(s) the employee will be working on, and the categories of technical information to which the employee will have access;

    e. must execute a non-disclosure agreement with Xerox, as discussed in section 3.4;

    f. may not take technical data out of the U.S. unless it has been logged, recorded, and approved in accordance with our export control regulations. A temporary visa employee who leaves the U.S. immediately reverts to the *foreign affiliate* status, with all its incumbent restrictions.

5. Foreign non-affiliates:

    a. may be given access only to *public-domain* information;

    b. must not individually be on the U.S. Government denial list or members of organizations or countries on this list.

    c. A record must be kept of all transfers of information to foreign non-affiliates except Canadians; this includes *all* technical information, even though in the public domain.

2. Organization of access controls

Now we review the mechanisms that exist for controlling access to electronic information in the Xerox Research Internet.

To begin with, it should be understood that the Internet is designed to permit any connected machine to communicate with any other, without any controls or restrictions. Since the Internet extends outside the U.S., this enables unrestricted international communication. Any required restrictions on information transfer are the responsibility of the end parties of the communication, not of the Internet.

2.1. Basics of access control

The principal means of ensuring that a certain piece of information can be accessed only by certain individuals is by attaching an *access control list* to the information and by requiring that individuals be *authenticated*. Let us consider what this means.

An access control list is simply a list of names of individuals who are to be granted access to the associated information. For example, a file stored on a file server has a *protection* which, simply put, is an access control list that determines who may access the file. Upon each attempted access, the file server checks the name of the individual requesting access against the file's access control list, and permits the operation to proceed only if a match is found. This is entirely the *server's* responsibility, though the server can delegate some of the work to other servers as will be discussed

shortly.

In order for this style of access control to be effective, it is necessary for the server to be able to determine that an individual's *name* actually represents that individual. This is the purpose of the *password*. The name and password together serve to *authenticate* the individual that is, to identify the user and to verify his authenticity by requiring him to provide some piece of information that only he knows.

It should be clear why it is vital that users choose passwords with care and keep them secret. In an access control list based protection system, access is granted solely on the basis of *who the requestor is*, and not on criteria such as the requestor's physical location, ability to supply a password for the information being accessed, or other credentials that the user might possess. An individual's name and password is intended to represent *that individual* and nobody else.

2.2. Individual names and authentication

In the Xerox Research Internet, an individual is identified by a Grapevine *registered name* or R-Name'' composed of two parts, a *simple name* and a *registry*, separated by a period. A registry is a logical grouping of names, usually on a geographical or organizational basis; and a simple name identifies a specific individual within the registry. Examples of R-Names are Smith.PA'' and Jones.EOS''. A complete R-Name uniquely identifies one individual. In the Xerox 8000-series products, R-Names are composed of three parts instead of two, but otherwise are organized essentially the same.

The Grapevine servers maintain, for each individual, a password and various other attributes. One of the services provided by Grapevine is to authenticate an R-Name and password.

When a user requests service from, for example, a file server, that server first demands that the user (or client program acting on his behalf) provide a valid R-Name and password, which it asks Grapevine to authenticate. This process of logging in'' serves solely to identify the user; by itself it confers no access rights. That is why any authenticated user is permitted to log in'' to any IFS. Control over the user's access to information is accomplished by an entirely separate mechanism.

2.3. Groups and access control

Grapevine also maintains *groups*. A group, to first order, is simply a list of R-Names. A group itself is identified by an R-Name (which customarily, though not necessarily, contains a ^'' character).

Groups are used as access control lists, as well as for other purposes such as directing the distribution of messages. If a group is attached to some piece of information as its access control list, then an individual can access that information only if his R-Name is included in the group. This is the fundamental basis for access control in IFS, as well as in Grapevine itself.

Groups can contain other groups; this capability can be used to model organizational hierarchies, project membership, and various other structures. By using an appropriate group name for access control, information may be made available to every member of an organization, project, etc., even though the actual membership of that organization or project changes over time.

Groups can also contain *patterns* such as *.PA''; any individual whose R-Name matches the pattern is considered a member of the group. This facility is provided as an administrative convenience in defining all-encompassing groups (and avoiding the need for exhaustive enumeration); but it does have certain consequences that will be discussed later.

Permission to change the membership of a group is itself controlled by access control lists. Some groups may be changed only by duly authorized managers of the organizations or projects which they represent. Other groups (the so-called interest lists'') permit any individual to add or remove his own R-Name.

The way this works is as follows. Each group has two access control lists called the *Owners* and *Friends* lists. An individual whose R-Name is in the Owners list is permitted to change the membership of the group arbitrarily (as well as to perform certain other operations). An individual whose R-Name is in the Friends list is permitted only to add or remove his own R-Name in the group's membership list. Centrally controlled groups have an empty Friends list, whereas completely uncontrolled groups have a Friends list of *'', a pattern that matches any R-Name.

2.4. IFS file protections

The preceding section described the general use of Grapevine groups as access control lists. The actual use made by IFSs is somewhat more complex.

Each file stored on an IFS has a *protection* consisting of two access control lists; roughly speaking, one controls reading and the other writing. Actually, there is a third list controlling appending, but that is of no relevance to the present discussion. Additionally, each directory on an IFS has a default file protection, which is applied to newly-created files in that directory. Finally, each directory also has two access control lists that control permission to *create* new files in the directory and to *connect* to the directory for the purpose of performing owner-like operations such as changing the access control lists themselves.

The group R-Names that may be mentioned in these access control lists are limited to a relatively small set that is chosen by the IFS's administrator. Thus it is the administrator's responsibility to ensure that only suitable groups are used as access control lists.

Each IFS also has a special access control list called World'' which represents some all-encompassing user group. For IFSs in the U.S., World'' is usually defined to be USRegistries^.internet, which consists of all registered Xerox employees and affiliates in the U.S.

The intent of this arrangement is that World'' be included in the access control lists of all files that are *proprietary* but are not in a more restricted classification (such as *private* or *registered*) and have no other reason for more limited access. This facilitates communication among Xerox employees. Foreign nationals located outside the U.S. (whether or not they are Xerox affiliates) and all non-affiliates are denied access to such files in conformance with the information security requirements presented in section 1.

3. IFS and Grapevine administrative policies

In this section we describe specific IFS and Grapevine administrative policies that are intended to ensure that the information security requirements are fulfulled. Note that these policies must be applied consciously by the administrators; they are not enforced automatically by the software.

3.1. Registry membership

Each Grapevine registry is typically maintained by a single person or a small group of specially-designated people. The registry maintainer has the responsibility for ensuring that only valid individuals are registered.

First of all, it is important to understand that there are two classes of registries: those that contain human individuals (and groups of individuals) and those that contain other names used for special purposes. All of the familiar registries belong to the first class, such as PA, ES, Wbst, etc. Registries in the second class contain individuals that do not represent human users but rather machines, programs, or processes; for example, the GV and MS registries, used for internal control over the Grapevine data base, belong to this class. These two classes of registries must not be confused, for reasons that will become apparent shortly.

With this detail behind us, we now state the first principle of Grapevine registry administration:

Z 1. Every individual R-Name registered in a normal organizational or geographical registry must correspond to a human user; and the R-Name is for the exclusive use of that user.

This rules out assigning individual R-Names for guest'' or communal use or for automatic'' access by programs that have such R-Names compiled into them. (This constitutes a major break with past policy. Situations for which such ficticious R-Names have been assigned in the past may be dealt with by the procedures described in section 4.)

Z 2. Every individual registered in a Xerox U.S. registry must be a U.S. employee or U.S. affiliate (i.e., a member of group 1 in the classification presented earlier) or a temporary visa employee or affiliate (group 4).

That is, every individual in registries such as PA, ES, and Wbst must be a U.S. Xerox employee or affiliate, or a Xerox foreign employee or affiliate working in the U.S. Non-affiliates and foreign affiliates must be segregated into separate registries. For example, there exist registries RX and FX containing members of the Rank Xerox and Fuji Xerox organizations. It is straightforward to create new registries for other categories of individuals.

The reason for this is that the registries themselves constitute groups whose names are the patterns *.PA'', *.ES'', etc; all individuals in these registries are members of their respective groups. The group USRegistries^.internet is defined in terms of these registry groups; its present composition is: *.DLOS, *.EOS, *.ES, *.Henr, *.LB, *.PA, *.STHQ, *.Wbst, *.XRCC. Since this is intended to describe all U.S. Xerox employees and affiliates, it is clear that individuals who are not U.S. Xerox employees or affiliates must not be assigned to these registries.

3.2. Group classification

There are three basic classes of Grapevine groups, characterized by their style of use:

1. Organization groups, which reflect the corporation's organizational hierarchy. Each individual who is a Xerox employee is ordinarily a member of exactly one organization group corresponding to that individual's immediate organization. That group is in turn a member of some larger group; and this structure continues up to the root of the hierarchy. An organization group may be modified only by administrators associated with the organization, to reflect new hires, terminations, and transfers.

2. Project groups, composed of members of individual projects. These frequently cut across organizational boundaries, and may have a hierarchical structure of their own. The membership of a project group is ordinarily controlled by the manager of that project.

3. Interest groups, which are ad-hoc collections of individuals who are interested in sharing information about some subject. The access controls on interest groups are generally arranged so that any individual can add or delete his own R-Name.

The distinction between project and interest groups is not always clear-cut. A good guideline is to assume that any group whose membership is centrally controlled by one or a small number of responsible individuals is a project group; all other groups are interest groups. Equivalently, any group whose Friends'' list is non-empty or whose Owners'' list is itself a group is probably an interest group.

With this classification in mind, we now continue with the registry administration policies.

Z 3. Do not permit interest groups to be used for IFS access control.

That is, an IFS administrator should not specify an interest group as one of the groups usable for access control on the IFS. This should be obvious: a group to which any individual can add his own R-Name is a totally ineffective basis for access control.

Z 4. On U.S. IFSs, do not permit groups containing non-affiliates or non-resident foreign affiliates to be used for IFS access control, except by prior authorization. Exceptions to this rule must be approved by the International Deputy (see section 5.1).

This is required to ensure that such individuals cannot gain access to information in violation of the security guidelines. Exceptions to this policy for specific projects and individuals may be authorized by the International Deputy on a case-by-case basis.

3.3. International information transfer

Under U.S. Government regulations, most transfers of information to foreign nationals (whether Xerox affiliates or non-affiliates) are required to be logged. Since no automatic logging mechanisms presently exist in the Xerox Research Internet, such transfers cannot be permitted via the Grapevine and IFS access controls. Instead, some more centralized and restricted procedures are required.

Note that this requirement applies to technical and business documents, but not to casual interpersonal correspondence conducted via electronic mail. The latter corresponds to first-class letters in the postal system, which are also not subject to any regulations. Of course, the distinction between a document'' and a letter'' is not clear-cut; the sender must exercise some judgement in determining whether it is appropriate to send a particular piece of information by electronic mail.

To ensure the necessary control, it is required that information transfers from U.S. organizations to foreign affiliates be coordinated by the Export Control Coordinator for the originator's organization. This will also ensure that the required records are maintained.

The mechanism for transfer is that dedicated IFS directories be established that are accessible for writing by the Export Control Coordinator and for retrieving by persons in the registries established for foreign affiliates (or preferably by the Technical Information Center of the foreign affiliate, which will then distribute the documents further as appropriate). The Export Control Coordinator will determine whether the file is cleared for transmission to the foreign affiliates, move the file to the dedicated directories, and log the transfer.

3.4. Temporary visa employees and affiliates

When a foreign national who is working in the U.S. under a temporary visa starts work as a part of a Xerox group, his Xerox manager must write a memo to his Export Control Coordinator, identifying the employee, his term of employment, and the categories of technical information to which he will have access (e.g., technical information relating to office information systems, Star, 9700, printing). This memo is intended to satisfy the requirements for a documented record of the technologies that have been transferred to foreign nationals. The category may be made as broad as is necessary to enable the employee to work effectively and without obstruction. The memo should carry the approvals appropriate for authorizing transfer of information to foreign subsidiaries, and a copy should be sent to the International Deputy.

The temporary visa employee or affiliate must also execute a non-disclosure agreement with Xerox at the time he starts work with his Xerox group. He must do this even if he has previously executed such an agreement with a Xerox foreign affiliate.

When a temporary visa employee or affiliate leaves the U.S. while remaining an employee or consultant of Xerox Corporation or an affiliate, his status immediately reverts to the foreign affiliate classification. In particular, he may not take technical data out of the U.S. unless it has been logged, recorded, and approved in accordance with our export control regulations; he may no longer be granted the broad access available to temporary visa employees or affiliates; and he may no longer be included in U.S. registries or in U.S. organization or project groups except with specific approval by the International Deputy. If the employee leaves the U.S. and ceases to be employed by Xerox or an affiliate, his status reverts to the foreign non-affiliate classification and he may have access only to *public domain* information.

4. Commonly-occurring problems

In this section we consider various situations that have arisen in the past and that have sometimes been handled in ways that violate the above policies. Historically such practices developed because the authentication and access control mechanisms were inadequate. Now that the Grapevine facilities are available, these practices are no longer necessary and should be abolished.

4.1. Communal R-Names

Sometimes R-Names are assigned for communal use by multiple people. Strictly speaking, this does not result in violation of any information security requirements so long as all users of the communal R-Name have exactly the same status (i.e., are members of the same organization and projects).

But there are many disadvantages to this. When no single user is personally accountable for use of the R-Name, it's hard to detect and control unauthorized use. When one of the users transfers out of the project or leaves Xerox, maintaining the R-Name's integrity requires changing its password, which inconveniences all the other users (with the consequence that the password usually doesn't get changed). It's hard enough for administrators to keep track of organization and project membership without having to worry about informal groups'' of users who share a single R-Name.

For these reasons, the policy of assigning an individual R-Name to each user should be rigidly adhered to. If a person has legitimate reason to use the Xerox Research Internet, then that person should be registered without exception.

4.2. Institutional R-Names

A related case is the one in which an R-Name represents not a particular person but some function, organization, or service; the R-Name is assigned for the convenience of people attempting to access the entity it represents, so they need not remember the R-Names of the individuals who actually embody that entity. Examples of such R-Names are LaurelSupport.PA and NetSupport.Wbst.

In this situation it is usually most appropriate for the R-Name to identify a *group* instead of an *individual*. The members of the group are simply the R-Names of the people representing the named entity.

Sometimes institutional R-Names have been registered simply so that messages can be sent on behalf of those institutions. However, this is not necessary, since Laurel permits the originator to specify the From'' and Reply-to'' fields of a message explicitly; for example, a member of the LaurelSupport group can compose a message that says it is From: LaurelSupport.PA''. In this case, Laurel adds a Sender'' field to identify the actual originator of the message.

4.3. Delegated access

Sometimes a user will desire to delegate access or authority to another person. For example, a user may want his secretary to read his mail while he is on vacation, or may want to make some private file available to a second person. Users sometimes give out their passwords to others under such circumstances.

This is *never* appropriate, and *always* violates the information security requirements. It should be impressed upon users that they are to keep passwords secret and never divulge them for any reason whatever.

An individual's incoming mail may be temporarily diverted simply by establishing a forwarding'' entry for that individual in Grapevine.

In general, users should be encouraged to work within the system when transferring information to others. If some individual does not have access to certain information, it is usually because the individual is not a member of some group that he should be in, or because the information's access

control list (file protection) has been set incorrectly. Smooth information transfer requires that people understand how the protection system works and how to use it.

4.4. Automatic access

A number of programs have been developed that access IFSs using a compiled-in R-Name and password instead of the credentials of the human user running the program; examples of such R-Names are Guest, ARUser, Librarian, and Smalltalk-User. The existence of such R-Names constitutes a security loophole, for reasons already presented, and they must be abolished.

Most uses of compiled-in credentials exist for no better reason than that the implementors of the software consider it too inconvenient to obtain the human user's credentials. Users are justifiably annoyed when they must log in repeatedly because the software they are running forgets their credentials in mid-session (e.g., because a new Pilot volume is booted); alleviating this annoyance is a likely reason for the widespread use of compiled-in credentials. But the resulting adverse impact on information security makes this practice no longer tolerable.

In a relatively small number of cases, such automatic'' access really is required because human interaction is impossible for some reason. For such applications, it is possible to establish individual R-Names representing non-human entities; but these R-Names must be in *special registries* that do not also include human individuals. That is, it is unacceptable for such R-Names to be in registries such as PA, ES, and Wbst. (For example, the existing RS and MS registries contain R-Names representing the individual Grapevine registration and mail servers.) A special registry, Auto'', has been created specifically for this purpose; to register an individual in the Auto registry, send a message to Registrar.Auto.

Access by such non-human individuals to information must then be precisely controlled by proper definition of groups and use of access control lists. Such individuals are not in any IFS's World'' group since their registry is not among the ones included in USRegistries^.internet; thus their credentials cannot be used to subvert the protections of proprietary information.

System implementors who elect to adopt this strategy should be aware that all information obtainable by such automatic'' means may also be accessed by *anyone* able to obtain a copy of the software (or discover the R-Name and password by other means), regardless of who or where he is, whether or not he is a Xerox employee, etc.

To summarize: a program accessing information on behalf of some human user must obtain and present that user's credentials without exception. Only when human interaction is *impossible* (e.g., in servers that run unattended) should credentials be compiled into programs or otherwise stored for later automatic use; but such R-Names must be in special registries (e.g., Auto) which are not included in USRegistries^.internet.

5. Additional information

5.1. People

Horace Becker (8*222*2163) is the International Deputy for Reprographics and Jerry Elkind (8*923*4610) is the International Deputy for Non-Reprographics. Each organization has its own Export Control Coordinator.

5.2. Documentation

More detailed information about electronic information security and proper use of the authentication and access control facilities is available from several sources:

1. Electronic information security guidelines’’, in the October 1981 issue of the Xerox Research Internet Newsletter.

2. IFS meets Grapevine’’, in the March 1982 issue of the Xerox Research Internet Newsletter.

3. How to use IFS’’, filed as <IFS>HowToUse.press on many file servers.

4. Maintain reference manual’’, filed as <Laurel>Maintain.press on many file servers.