Report on Critical Issues: Museum Security
and Fire Protection, January 14-18, 1991

The Critical Issues course in 1991 was held at the Smithsonian in Washington, D.C. with project field trips to Arlington House and Ford's Theater. This course was multi-discipline with a good mix of curators and protection rangers at all levels. It was the kick-off for the new security/fire protection funds which were available starting in FY 91. This report was part of our post-course assignment to provide a written report and/or discuss the course content with park management and staff. It has been revised for distribution with the Curatorial newsletter. Many of the ideas may seem unrealistic or not applicable to your park but there may be some good ideas for you to consider. If you have any questions, please call Jane M. Sundberg at FTS 920-3400, ext. 56 or commercial (804) 898-3400, ext. 56.

Session I: Introduction

Ann Hitchcock, Chief Curator, introduced the course by giving a summary of the museum security and fire protection needs identified by the parks in Special Directive 80-1. For example, out of 294 park units which completed 80-1, 87 parks reported deficiencies in key control, 151 reported deficiencies in incorporating their collections in Emergency Management Planning and 200 reported that they needed security surveys (the thrust of this course). Ann talked about the cataloging funds which have been available since FY 88. These are expected to remain in the NPS base budget at $2.5 million per year (at least through 1996). FY 91 was the first year for the next thrust (security) and there was $1.6 million available. $2.6 million was budgeted in FY 92 for security and this, like cataloging, is expected to continue.

Walt Dabney, Chief of the Ranger Activities Division, also spoke. He stated that the NPS is the third largest federal owner of buildings and for the first time in its history, the NPS now has a structural fire specialist (Jim Farrell who is with the Branch of Fire Management in Idaho). The division was also hoping for a position and $3 million in funding to coordinate the archeological looting prevention program.

The strength of the course was rooted in the credentials, experience and fluency of the presenters. These included John Hunter, NPS expert on security and fire protection; Bob Burke, Director, Office of Protection Services, Smithsonian (for facilities worldwide); Steve Keller, Keller and Associates; and, Danny McDaniel, Director, Security and Safety, Colonial Williamsburg Foundation. They were backed up by the security and fire protection staff of the Smithsonian as well as some NPS staff. The Smithsonian staff, Steve Keller and CW's Danny McDaniel showed a good understanding and appreciation of collections and the concerns of curators. However, in my opinion only Colonial Williamsburg's collections and structures were similar to NPS sites. The Smithsonian collections and the

valuable art collections that Steve Keller works with require professional security staffs whose duties include what NPS interpreters or even volunteers do (such as opening and closing buildings, checking on exhibited objects, etc.). Also, they are more building oriented. However, despite these types of differences, the sessions were very applicable to NPS.

I felt that the course topics and the interaction of the members of the class demonstrated that the NPS has a lot of work to do in bringing curators and protection closer together especially in our attitudes towards each others' jobs and responsibilities. Although we did not have any of the Smithsonian curators speak on their relationship with security, security did mention many times the differences they have with curators and how both groups must compromise. Bob Burke particularly cautioned on the need for protection and curators to learn each other's language. He felt that differences in word usage and jargon between the two disciplines can alienate or lead to misunderstandings.

Part of the first session was a pre-course assignment to describe cases of theft or fire in the participants' parks within the last five years. The range of examples was enlightening but too long to list here. The following list describes why such incidents occurred: lack of training, faulty design/construction of exhibit cases, lack of staff, no or insufficient alarm systems, staff attitude, mechanical system complexity, lack of funding, lack of documentation/reporting procedures (including failure to report or gloss over an incident), problem of communication among divisions, policy deficiencies and/or conflicts, policy priorities, and varying levels of protection.

Session 2: Selling Security to Management

Bob Burke gave a good session on "Selling Security to Management." It must be remembered, however, that the types of management situations he deals with at the Smithsonian are different than the NPS. But there were many thought provoking ideas. Basically, he recommended taking advantage of emergencies and thefts to get projects done. Maximize the disasters of others. Concentrate on selling the pay-offs of the project; especially how it will save funds and avoid bad public relations in the long run.

Bob Burke also recommended motivating staffs to want security and to get them into a security routine. But, he warned, don't be oversold by security companies. Do not use companies who are product affiliated to conduct surveys for you or to recommend security needs as they will gear it to their products only. Security is both operational procedures and equipment. Too often we put too much emphasis on the equipment. Put recommendations to management in writing and request a specific response. The decision on whether or not to follow through then becomes

management's responsibility. [Based on the Federal funding process, I would think this approach is easier with Boards of Directors who have some direct control of funds.]

Session 3: Risk Identification and Assessment

This session was presented by Steve Keller. Risk management is the process of assessing threats and the likelihood of a specific threat happening at a specific site. It is a tool for deploying limited resources. It is recognizing, identifying and controlling losses to persons and property. The five methods of management are 1) risk avoidance (keep it from happening), 2) risk transfer (insurance or making it someone else's problem), 3) risk reduction (apply security and preventive measures), 4) risk distribution (make threat less critical-- such as back-up tapes for computer data), and 5) risk acceptance (grin and bear it, a way of dealing with low value items). Steve recommended two basic methods of assessment. One is a software program called Rank-it whose main advantage is that it allows a long list of comparative ranking in a short period of time. Steve's preference, however, is for the "John Hunter Method" which uses a chart (distributed to the class) to identify risks, and evaluate risk history, probability, and criticality. The parks need a team to do this and the parks need to prepare a loss history record including but not limited to law enforcement files; interviews with past employees, volunteers and neighbors; archival and newspaper files; civil defense records and weather service records.

Session 4: Operational Security

Steve Keller also presented this session. Generally, it is felt that operational security can take care of most of our security gaps and is the cheapest method. So, look at your park's operations before going with electronics. There are three main elements: access control, parcel control and internal security. Access control includes key control, providing physical barriers, locking cases and cabinets and controlling the terrain around the site. Written procedures are essential for all access control. Parcel control includes checking parcels (of course, check rooms are not plausible at National Parks) and examining parcels (including being aware of what goes out of the mail room). The subject of internal security led to a long discussion on background checks (cans and can'ts) on employees and even a suggestion that curatorial staff should be bonded. It was recommended that security training should be given to all employees (including seasonals).

This session brought out a lot of interesting tidbits for us to consider. Researchers using the archives are of particular concern. Some museums have the researchers sign a statement that

they are aware of electronic and staff surveillance and that they do not object. This in itself can deter theft. Parcels larger than 11 x 14 should be restricted. Outgoing parcels and briefcases should be examined. Contractors need to be controlled as it is easy for them to carry materials in and out of buildings. The mail room is an easy way for employees and researchers to mail out items taken from the collections. Many of these situations do not necessarily apply to our park situations but we need to be aware of them. According to statistics about 90% of the security problems are internal.

The operational security session also touched on electronic security which is covered in greater detail in Sessions 7 and 10 below. In regard to electronic security, several recommendations were made. If we use electronic locks on collection rooms, we should also have deadbolts as electronic systems can be bypassed. The use of facilitrac was preferred over the Best system as it was felt (by some) that Best does more than is necessary. Facilitrac is supposed to be listed in Bell Atlantic but I could not find it. John Hunter has more information on this system. Also, all new exhibit cases should be prepped for alarm installation. Exhibit case construction was seen as a major issue. Consider installing local audio alarms in exhibit rooms. Light Impressions sells a inexpensive lock for hanging paintings on walls.

Session 5: Physical Security

This session consisted of a panel of Smithsonian security staff. The first point they stressed was that everyone considers security to be fine as long as it benefits individuals but does not inconvenience them. [Of course, none of us is guilty of that perception!]. The panel also stressed that more important than security is the appearance of security.

[As an aside to this discussion, there was a short discussion on evacuation plans. The Smithsonian has incident command centers in each of its buildings. There are sufficient phone jacks installed in the designated area and each area has a roll cart with all information and equipment stored in it (blueprints, guidelines, inventories, telephones, television, flashlights, etc.) for immediate use. I felt this was a good idea for our museum disaster plans as well.]

It is important for the curators to train the protection staff on the collection rooms and exhibit areas and there should be a policy statement concerning law enforcement drills in exhibit areas. For instance, at the Smithsonian no drill actions may threaten the exhibits and a curator has to be included in the drill. In case of a theft from the collection or exhibit, the interpreter or curator should protect the scene (cordon it off)

until protection arrives. No one (including volunteers) should discuss the value of the collection or the security of a site.

The panel discussed the six levels of perimeter security. Perimeter security is the concept of concentric rings of security with the highest security in the center. At the center is the alarmed vault with very high security for both fire and intrusion. In the case of art museums, this area is restricted to curator access only. However, in most parks the "center" is an alarmed security storage room under the control of the curator but with limited access to others (the second ring of security in the diagram). Additional rings moving outward are the curatorial workrooms; offices; exhibit areas; public areas (restrooms, lobby, shop); and grounds. Each of these areas should be evaluated for its level of security.

Some additional notes from this session include: keys for limited access areas should never leave the building (signed out as needed); in large storage areas, the use of chain link fences can isolate areas which need greater security instead of building walls; keys in sealed envelops countersigned by the curator can be used for emergency access; researcher/visitors sign-in sheet must have name printed and an identification number of some sort; sign-in sheets should be put in the archives (for future use in incidents); logging the path of movement of an artifact is important (the paper trail history); make sure when ordering museum storage cabinets that different keying systems are requested (otherwise standard key system will be used making keys from other sites useable on your cabinets); for glass display cases (storage primarily but also possible in some exhibits) put acid free paper on the bottom and draw the outline of the object so can immediately see if it has been moved or is missing; temporary storage areas never get the same security attention as permanent areas and yet they frequently end up becoming long term storage and, therefore, more vulnerable; need to set up a system during opening and closing to include a sweep of the exhibits to check if anything is missing; doors with outside hinges are one of the greatest security risks; doors should have automatic closers; key boxes should have standard key lock plus a combination lock.

Session 6: Security Surveys

The session on security surveys was presented by Danny McDaniel of the Colonial Williamsburg Foundation. Because of their size and complexity, CW does their survey in sections. The emphasis of the entire course was the need to complete security surveys before investing in security and fire protection systems. The surveys are important for identifying both operational and electronic needs.

The objectives of the survey are:

1. Understand the existing system, know what you have and find out if you actually have a system, whether everyone actually knows what is system is and who has responsibility. Does everyone have the same interpretation of the system?
2. Identify potential threats (goes along with disaster planning threats list)
3. Identify appropriate countermeasures to the threats (broad range)
4. Analyze appropriateness of existing countermeasures
5. Identify modifications needed to fit existing countermeasures to existing threats
6. Identify resources needed to improve security system
7. Develop an implementation plan
8. Results of survey should be used as an education and awareness tool for management and staff. The security survey is good training for new protection staff as well as other park staff.

Steps for understanding the existing security system

1. What do you have on paper?
2. What do you have in practice?
3. If 1 and 2 are different, why? (Changes in procedures? Was only one division/individual responsible for writing procedures?)
4. Who is responsible and for what?
5. How do you know when it is being done when it is, and how do you know when it is not? What are the feedback loops?
6. How does a new employee coming in learn about the requirements?
7. How effective is the current system?
8. How is effectiveness measured? Are the statistics realistic? How much of the effectiveness is the result of luck (good or bad)?
9. How does the system adapt to changing threats?

Preliminary Preparations for a Security Survey: This is the most time consuming and important task. Prepare a task directive.

1. Make sure there is Management support, that everyone <u>understands</u> and <u>agrees</u> on the objectives and the priority of the objectives. Make sure everyone has the same definition of security before making recommendations.
2. Identify objectives
3. Determine the nature of the facility; what is in it, how is it used?
4. Assemble team; must be broad based; assign members to task groups; 6-8 people are needed.
5. Identify and obtain adequate resources (enough staff time

for site visits, meetings and preparing reports)
6. Develop a schedule; complete a written report. Use task groups to look at specific issues and write reports. The overall team meets 4-6 times.
7. Get the task groups to present their findings to Management. Include minority reports on issues if necessary.

You do not want anything to happen on your site that you did not anticipate and make plans to prevent. Accept loss if necessary but on your own terms. This is a good argument for management support. You need to determine what is an acceptable level of loss. What is the bottom line? Make sure you articulate this.

Remember, security is part of museum conservation. It is not a separate process.

Conduct a site survey (best to conduct during a high visitor use time).

1. Interview key personnel
2. Inspect facility: site, perimeter, access control, access during all types of weather, opening and closing procedures.
3. Protection of the collection: access to collection; objects inventory and accountability.
4. What is security awareness of staff?
5. Is staffing adequate to protect high value objects?
6. What are crime prevention measures?
7. What are cash control systems?
8. Facility electronic protection
   - -who responds?
   - -length of response time (if it takes 35-40 minutes then alarm system is not worthwhile)
   - -reliability of response (is there always a response?)
   - -what do they do when they get there?
   - -factors that inhibit response
9. Prepare the report for site
   - -Task Groups submit reports
   - -Team discusses task reports
   - -Team agrees on findings and recommendations
   - -Team Leader prepares draft report and submits to team for comment
   - -Reconcile comments or have dissenters prepare minority reports for inclusion in final report
   - -Submit final majority report and, if required, minority reports to management and schedule a time to present the report

Session 7: Introduction to Electronic Security

Just a few notes on this. Glitton shock sensors are simple, non-intrusive devices for windows (careful of rattling windows). The

problem of devices for protecting pictures is that they protect the frame, not the canvas.

Session 8: Field trip to Arlington House

Sessions 9 & 10: Physical Security Hardware (hands-on)

These sessions were conducted by several of the Smithsonian staff headed up by Chief of Security Systems, Warren J. Danzanbaker. These sessions provided literature and demonstrations of the large variety of hardware (past and present).

There were some valuable notes from this session.

*Strongest recommendation: keep equipment simple
*The crowbar is still one of the most effective methods of breaking in.
*Battery run drills now make picking locks easy.
*Most hasps for padlocks can be broken with a screw driver. There is a tendency to put on a good padlock and a cheap hasp.
*No outside hinges.
*For museum storage: always have self-locking lock; double lock with a 1" deadbolt; if a latch is used then put in a latch guard (if you can see the latch then you can defeat it); always use a steel door and steel frame.
*no temporary employee should get keys to take home and must sign out key on a daily basis (not always practical for NPS).
*Most key boxes can be easily entered; need to use one with a combination and key lock.
*Most efficient if inhouse staff can be trained to re-key locks.
*John Hunter recommended that key devices (such as Best) used for the rest of the park should not be used for museum storage; have two different systems.
*It was recommended that Medeco is the best cylinder.
*If a card system is used make sure there is a back-up deadbolt in case the card system fails (otherwise will not be able to lock up collection).
*All keys should be stored by code and not by location number.
*Information on key distribution should be kept on the computer (dBase) so that can get a printout each year for status, statistics.
*The benefit of the card system is that the cards can be issued for certain days and hours and can be changed immediately in case of loss. Also, cards can be reused by others. Newer card systems have terminal processors which make the decision and are linked to a PC. If the PC crashes you will not lose the capability to open the lock.
*Digital alarms are dependent on the telephone line and the telephone line can be cut or go down. Therefore, there should also be an alarm bell outside the structure.

****

Security devices for exhibits and exhibit cases were also covered.

*Consider the installation of ultrasonic devices in the exhibit case (can paint it same color as case to make it invisible). Remember to install the devices so they face the longest way so ultrasounds don't bounce back from too short walls.
*Consider the use of motion detectors (local and central alarms) in exhibit rooms.
*Most detectors will cost under $70.
*Consider the use of personal emergency transmitters to be worn by curators working alone (Smithsonian now does this after a museum case fell on a curator)

*There are new (not on market as of January 1991) wireless transmitters which can be attached to the back of paintings.

NOTE: The Smithsonian demonstrated the "new" water alarm system we use in Washington's Tent. They use these in construction areas where flooding is a possibility (however, these areas are also patrolled at night so an active alarms would be noticed).

Sessions 11 & 12: Fire Protection and Prevention

These sessions were conducted by Andy Wilson, the Smithsonian's Chief of Fire Protection.

Andy strongly supports the use of water suppression systems in museums. Sprinkler systems can be zoned and the amount of water in the lines regulated. There are an average of 102 museum fires a year (reported) but the degree of these fires is unknown. Once a fire has to be fought from outside the building then the terrific weight of water trained on the building (5000 gallons per minute) will destroyed just about everything.

*Smoking is fairly high on the list of reasons for fires. Museum must have a written policy.

*Construction tools are the highest fire risk. There should be a written policy regarding construction. The Smithsonian requires a permit to be signed.

*Portable heaters, coffee pots, toaster ovens, hot plates and similar appliances must be controlled. They should be approved and set up away from all combustible materials. The Smithsonian said that their situation got so bad they now only permit commercial quality appliances that have "on" indicator lights and automatic shut offs.

*Make sure that carpet, curtains, etc. are fire retardant. Wood should be pressure treated with the retardant impregnated into the wood (often difficult to get). Surface coatings including retardant paints are not all that effective.

*Reproduction fabrics can be treated with a home brew (contact Smithsonian for the formula).

*Ask manufacturer for data sheets on fire retardant capability, how combustible and how fast fire would move (this to be used as part of survey information).

*Exhibit panels should be treated.

*Try to break the building into fire zones

*Make sure that open stairwells are enclosed in some way.

[The Smithsonian Fire Protection Division is available for advice and assistance to the NPS (Andy Wilson, FTS 287-3613).]

Andy summarized the different types of systems and their uses:

*Ionized detectors are best for small particles usually given off in the flame stage.

*Smoldering fires are best handled by photo electronic detector (based on light scattering principle).

*Beam detectors are good for historical structures and for covering large areas. They can go on the wall and fewer are needed. NOTE: All the session speakers were sensitive to the needs of museums and historic structures and to have systems that would not be visually intrusive. At the same time, it was stated that there has to be quite a bit of compromise on the best system/least intrusive system. The Smithsonian, of course, has the inhouse staff to develop custom made systems when necessary.

*Heat detectors are good in kitchens or in shops where smoke alarms would become a nuisance. There are varieties which react to a set temperature or react to a rapid change (15 degrees) in temperature.

*The hand held fire extinguisher is the ideal situation and all staff must be regularly trained on these. BUT, always report fires before trying to put them out.

*Systems are becoming more sophisticated. It was noted that Honeywell is not a good system for museums due to the small number of manufactured items and the lack of emphasis on maintenance.

*Some manufacturers have insect screens. Otherwise don't use deep detectors. Insects in systems are a big problem.

*Hochiki is a Japanese manufacturer with the smallest reliable detector (good for historic structures).

*The Mt. Vernon system is custom-made.

*Make sure to cover detectors during construction periods but the covers must be removed at the end of each day (put this in contract).

*Do not install detectors and heads in high, hard to reach places as they will be difficult to test or cover during construction. The Smithsonian installed them in the ceilings of galleries several stories high and it is a major (and expensive) effort to check them.

*Most halon is being phased out in the U.S. by 2000. There is now a $20.00 per lb. tax on halon.

*The only fire without water damage is the total loss fire (unless the system is halon). The pressure from water hoses is extreme and covers the whole building. A sprinkler system with local zones will produce much less water. All heads do not operate at the same time. Each one is heat activated. There will be far less damage from a sprinkler system than from fire department hoses.

*Statistics show that sprinkler heads are the most reliable mechanical systems in a building. There is a 1 in 16 million chance of an accidental dump (based on insurance figures).

*For museums and historic structures, the pre-action sprinkler system is good. The pipes stay dry under pressure until a head opens (due to a fire) and releases the pressure allowing the water to flow into the pipes and open heads. The drawback of this system is that it is more elaborate and gives a fire more time. Andy Wilson felt that the wet pipe system is slightly more reliable because it is a simpler system.

*Sprinkler systems can be controlled to limit the amount of water released.

*Aesthetically, the sprinklers can be adjusted so that only 1/2 or 3/4 of the heads are exposed. There are also side wall units which are just as effective. The technology is constantly improving and sprinklers are smaller and less intrusive.

*Sprinklers need 7-15 lbs of water pressure at the upper most sprinkler head (if working from a well). This is 15-20 gallons

per minute. You can now use plastic pipes (good for historic buildings as can use smaller diameter). [Check with Smithsonian on how their architects covered pipes in historic houses].

*The Smithsonian uses halon and would not use water in certain cases such as the Washington Tent. Sprinklers are also used where computers are located. It was observed by Jim Farrell (NPS Structural Fires) that there is should be little or no damage to the computers if they are cleaned within 72 hours.

Jim Farrell also emphasized the need to keep statistics on fires in structures in order to build a data base for funding needs. He also recommended designating a staff person who will call the fire department despite an automatic alarm.

Session 13: Field Trip to Ford's Theater

Session 14: Incident Reporting

This session was not particularly successful as the FBI representative scheduled to make a presentation canceled (this was the week that the Gulf War started). Unfortunately, the NPS presenter seemed to create an us/them atmosphere between protection and curatorial. My impression was that the presenter really was not too interested in the topic and the class reaction was rather negative. Two suggestions worth considering came out of the class discussion. First, if possible, the curatorial staff should see the morning reports as there have been cases where the curatorial staff was aware of similar CRM/Curatorial incidents which helped Protection. Second, all divisions involved should fill out an incident reports. Apparently, many incidents are never reported due to embarrassment.

Session 15: Integrating Museum Security

This session was conducted by Danny McDaniel, Colonial Williamsburg. He stressed that you must have a functioning program; it is too late when you are in the emergency to develop a program. Danny used the DeWitt Wallace Gallery flood as an example. (The DeWitt Wallace decorative arts museum is partially underground and was flooded during a freak rain storm which dumped 7 inches of water on Williamsburg in two hours).

1. It is best to keep objects on platforms and dollies. This is a security, not just a conservation measure.
2. All staff needs basic training on handling objects. In an emergency, the park will use everyone available.
3. In an emergency, the well-meaning staff is going to want to do more than it ought to. For instance, don't walk in flood water in bare feet or improper shoes; do not use electrical appliances in water areas (drills, fans, etc.).

4. Under stress, people will fall back on first learned behavior and instincts. Therefore, do not make major changes in your emergency procedures after everyone is trained unless absolutely necessary.
5. Panic occurs when there are no clear choices. Therefore, your emergency program should function on fundamentals while other usually required procedures will be dumped. For instance, in an emergency, no one is going to adhere to the curatorial requirement to wear gloves when handling an artifact. Make sure that the most important actions are emphasized.
6. The staff must feel they "own" the system that they are a part of. You can reinstate regulations when the emergency is over.
7. The system must be flexible to handle changes. It is the staff that will make the system work and <u>they must have the training and authority to take over.</u>

<u>Session 16: Wrap-up</u>

The wrap-up session was conducted by Ann Hitchcock and Tony Knapp. Ann reviewed the security funds which have been allocated to the regions and the priorities for funding based on the Special Directive 80-1. The highest priorty for the funds will be for parks to purchase insulated file cabinets for storing museum records. Fire and security systems are the next priority.

However, parks should consider fire protection and security survey before investing in such systems. Tony Knapp once again summed up the process:

1. Identify the risks and threats
2. Identify operation procedures (short term and long term survey comes into this category)
3. Identify physical security needs
4. Identify electronic security needs (there is a tendency to put this first to solve a problem when we need to do steps 1-3 first).