



# Navy Public Affairs Guide

## Public Release of Information and Imagery



3	<b>The Navy's Approach to Public Release of Information and Imagery</b>
6	<b>Security/Operational Security (OPSEC)</b>
8	<b>The Freedom of Information Act (FOIA)</b>
11	<b>The Privacy Act</b>
13	<b>The Health Insurance Portability and Accountability Act (HIPAA)</b>
16	<b>Copyright</b>
19	<b>Defamation</b>
20	<b>Considerations Unique to Imagery</b>
21	<b>Considerations Unique to Visual Information Products</b>
22	<b>Investigations / Accused Individuals</b>
23	<b>Criminal Activities and Arrests</b>
24	<b>Prisoners of War (POWs) – U.S. Forces</b>
25	<b>Persons Under Control (PUC) / Enemy Prisoners of War (EPWs)</b>
26	<b>Counter Narcotics Operations</b>
27	<b>Base Realignment and Closure (BRAC)</b>
28	<b>Scientific and Technical Information (STI)</b>
29	<b>Congressional Inquiries</b>

# Navy Public Affairs Guide

## Public Release of Information and Imagery



### The Navy's Approach to Public Release of Information and Imagery

Accurate, truthful, and timely communication increases the credibility and transparency of the Navy and enhances the legitimacy of our operations. Conversely, deceit – often the mere perception of such – significantly damages and undermines the trust and credibility the public places in our organization. While release of information and imagery is a command responsibility, it is often delegated to the public affairs officer. Navy public affairs professionals play an important role in maintaining public trust by advocating transparency and by preparing and reviewing information and imagery for public release in a timely manner.

**Navy public affairs professionals play an important role in maintaining public trust by advocating transparency and by preparing and reviewing information and imagery for public release in a timely manner.**

With the advances in communication technology and how we receive information, once information or imagery is released, there is no getting it back. Information and imagery released to an internal audience quickly may make its way to external audiences and vice versa.

The Navy's standard approach is to release information and/or imagery when it deems one or more of its audiences should know the information or when one or more of its audiences requests information. This default position, with due respect to categories of information and other certain circumstances identified here, is consistent with the DoD Principles of Information requirements for timeliness, accuracy and full disclosure.

The Navy makes information and imagery fully and readily publicly available consistent with statutory requirements, unless precluded by current and valid security classifications, privacy regulations or business proprietary guidelines. Information will be made available without censorship or propaganda and will not be classified or otherwise withheld to protect the government from criticism or embarrassment, when the information itself is unclassified.

Applicable laws and DoD and DON policies, including the Freedom of

Information Act (FOIA), the Privacy Act and the Health Information Portability and Accountability Act (HIPAA), will be supported in both letter and spirit.

Navy public affairs professionals present the facts and accurate information, which promotes a sense of trust and increases the Navy's credibility with internal and external audiences alike. Distorting facts and or disseminating inaccurate information are prohibited.

Navy public affairs professionals shall make every effort to maximize disclosure with minimal delay. Difficult issues and events potentially unfavorable to DON should be addressed openly, honestly, and as soon as possible. In the instance of accidents or incidents that require an operational report (OPREP), the PAO will submit a proposed news release with the best releasable facts available to the designated PA office within 1 hour of the release of the OPREP. The proposed release will be reviewed and will be edited, if necessary, before public release.

An important consideration in these matters is weighing, in some circumstances, whether the interests of the public or the Navy lead to greater disclosure than may otherwise occur. This is essential to maintaining the public trust and can apply to a variety of situations such as to operations when the information is critical to the audiences' understanding of why the U.S. is taking certain actions or to holding senior officials accountable. This "balancing" of public, institutional and individual interests is a matter of due diligence and requires an objective assessment.

**There can be negative consequences of holding onto information. Here are some reasons to release information as early as possible:**

The U.S. public, Congress and the media are entitled to "truthful, timely and accurate" information about the military, per the DoD Principles of Information.

Early release of information sets the pace and tone for resolution of a problem.

If you wait, the story will often leak anyway. When it does, you jeopardize trust and credibility – yours, the command's and the Navy's.

You can better control the accuracy of the information if you are the first to present it. If the story gets out incorrectly, it will remain incorrect.

There is more likely to be time for meaningful public involvement in decision-making if the information is released promptly.

Prompt release of information, including visual information, about one situation may prevent similar situations elsewhere.

Less work is required to release information early than to respond to inquiries, attacks, misinformation, etc., which might result from a delayed response.

If you wait, publics may feel angry and resentful about not learning of the information earlier.

People are more likely to overestimate the risk if you hold onto information.

## What Constitutes Public Release of Information and Imagery

The evolution of communication technology provides us with more ways than ever to quickly and easily release information and imagery to the public. Some of the most common public release mechanisms used by the Navy include:

- Press releases/press advisories
- Press conferences/briefings
- News stories posted to Navy.mil and command Web sites
- Photos and videos posted to Navy.mil and other official Navy Web sites
- Information posted to official Navy Web sites
- Posts to external official presences (EOPs) on social media sites, such as command
- Facebook pages, Twitter feeds, Flickr, YouTube, VIMEO, Issue, SlideShare and similar Web sites
- Navy magazines, newspapers, newsletters and familygrams (and associated Web sites)
- Welcome Aboard brochures
- Fact sheets
- Posters and flyers
- Visitor briefings
- Speeches
- Command Web site content
- Cruisebooks

This guide applies to all public release of information and imagery regardless of the medium in which it is released.

## Primary considerations when reviewing information and imagery for public release

As a Navy public affairs professional, you need to review every item for public release with an eye to two categories of criteria. Look at all items for public release from a technical standpoint first. Does the news story follow Associated Press, DoD and Navy style guidelines? Is it clearly written? Are photos in focus and properly exposed? Are videos clear and crisp and in a format that others can view? If the item is not technically acceptable, then the second will not matter in most cases. (Note: in some cases, content trumps technical quality. An image from cell phone shot by a Sailor without professional skills or training may be the only photo that tells an important story visually and should be considered for release.)

## Laws and Policies Governing the Release of Information and Imagery

There are a number of U.S. laws as well as DoD and Navy policies which govern the public release of information. The key ones to be familiar with when reviewing any information and imagery for release are:

- Security/Operational Security
- The Freedom of Information Act (FOIA)
- The Privacy Act
- Defamation
- Copyright
- The Health Insurance Portability and Accountability Act (HIPAA)  
(<https://www.hhs.gov/ocr/privacy/>)  
DoD 6025.18-R,  
DoD Health Information Privacy Regulation

# Security/Operational Security (OPSEC)

Information must be reviewed and approved at the appropriate level before release. Classified aspects of equipment, procedures, and operations must be protected from disclosure because of potential jeopardy to future operations, the risk to human life, possible violation of host nation and or allied sensitivities, or the possible disclosure of intelligence methods and sources.

## WHAT TO WATCH FOR WHEN REVIEWING INFORMATION AND IMAGERY

When reviewing content for release, Navy public affairs professionals ensure that the information or imagery does not compromise operational security. Photographers and videographers must take care not to inadvertently include classified weapons, maps, charts or systems in the background when shooting in operational areas. The following guidelines apply unless otherwise specified.

### The following information is **GENERALLY RELEASABLE**:

- Confirmation of ships and aircraft plainly visible to the public. Ship and unit departures and arrivals are generally of high visibility due to family involvement or other reasons. Guidelines for the release of departure and return dates are usually specified by the echelon 2 commander
- Approximate size of friendly forces embarked aboard ships and aircraft (exact numbers of forces or complete lists of units will normally not be provided)
- Casualty figures aboard the embarked vessel or aircraft (names will not be released until confirmation of notification of primary and secondary next-of-kin plus 24 hours subsequent to that confirmation has passed. Names may not be released even after notification if such release may endanger or hinder rescue or recovery operations)
- Results of completed missions
- Types and general amounts of ordnance expended (e.g., more than 25,000 pounds of high-explosive ordnance dropped from air wing)
- Number of aerial combat missions flown in the area of operations

### The following information is **GENERALLY NOT RELEASABLE**

unless declared otherwise by applicable public affairs guidance (PAG) or higher operational authority, or declassified for public release:

- Future plans or operations, including cancelled plans or operations.
- Specific numerical information on fleet or troop strength, aircraft, weapons systems, on-hand equipment, or supplies available for support of combat units. General terms should be used to describe units, equipment, and or supplies.
- Specific operating methods or tactics (e.g., offensive and defensive tactics or speed and formations). General terms such as “low” or “fast” may be used.
- Rules of engagement
- Security measures, force protection, or deceptive actions used as part of the operation;

- Intelligence collection activities (past and present), including intelligence methods, targets, and results
- During an operation, specific information on friendly force troop movement or size, tactical deployments, and dispositions that would jeopardize OPSEC or lives. This would include unit designations and names of operations.
- Detailed information about vulnerabilities or weaknesses; including information on the effectiveness or ineffectiveness of weapon systems and tactics (to include, but not limited to adversary camouflage, cover, deception, targeting, direct and indirect fire, intelligence collection, or security measures).
- Locations and activities of special operations forces, and their unique methods, equipment, or tactics, which, if disclosed, would cause serious harm to the ability of these forces to accomplish their mission.
- Identification of mission aircraft points of origin, other than as land or carrier-based.
- Information on operational or support vulnerabilities that could be used against U.S. or allied units until that information no longer provides tactical advantage to the adversary and is therefore released by the joint force commander. Damage and casualties may be described as “light,” “moderate,” or “heavy.”
- Information and imagery that would reveal the specific location of military forces including in imagery metadata and EXIF files or show the level of security at military installations or encampments. For datelines, stories will state that the report originates from general regions unless a specific country has acknowledged its participation.
- Information about downed aircraft or ships while search and rescue operations are being planned or in progress unless clearly in plain sight of media
- Specific types of ordnance expended, and (in some cases) the methods
- Location and activities of special operations forces
- Details of active law enforcement investigations.

# Freedom of Information Act (FOIA)

The Freedom of Information Act, codified in Title 5, U.S.C. § 552, allows an individual, a private organization or company, or a local, state, or foreign government to seek access to records, documents, and reports under the control of the Executive Branch of the federal government, such as those held by the U.S. Navy. Passed in 1966, it was the first law to establish legal right of access by the public to government information. Ultimately, the law protects the public's right to know and prevents excessive government secrecy.

In 1996, FOIA was amended to include provisions that address digital information. The Electronic FOIA Amendments expanded access to documents and records regardless of form or format and required that each federal agency create an "electronic reading room" available for public access on the World Wide Web for items of public interest to include:

- "final opinions [and] . . . orders" rendered in the adjudication of administrative cases
- specific agency policy statements
- certain administrative staff manuals
- records disclosed in response to a FOIA request that "the agency determines have become or are likely to become the subject of subsequent requests for substantially the same records"

Under FOIA, the Navy is required to disclose records upon receiving a written request, except those records that are protected from disclosure pursuant to nine exemptions and three exclusions. Even with the exemptions, the presumption today is in favor of disclosure. When applying the exemptions, consider whether one can reasonably foresee that disclosure would harm an interest of the Navy protected by one of the exemptions. In the absence of such harm, making a disclosure of the information is in keeping with being as transparent as possible. While Navy commands often use a separate office to manage the FOIA process, it is critical that Navy public affairs professionals understand the provisions and application of the law, particularly in the conduct of public engagement strategies. Below is a list of the exemptions and exclusions under FOIA. Keep in mind, properly determining what constitute one of these exemptions or exclusions is complicated work. Do not try to apply the FOIA law yourself. Consult your FOIA processing office for Judge Advocate for assistance.

## FOIA Exemptions

- classified national defense and foreign relations information
- internal agency rules and practices
- information that is prohibited from disclosure by another law
- trade secrets and other confidential business information
- inter-agency or intra-agency communications protected by legal privileges
- information involving matters of personal privacy
- certain information compiled for law enforcement purposes
- information relating to the supervision of financial institutions
- geological information on wells

## FOIA Exclusions

- Subject of a criminal investigation or proceeding is unaware of the existence of records concerning the pending investigation or proceeding and disclosure of such records would interfere with the investigation or proceeding
- Informant records maintained by a criminal law enforcement agency and the individual's status as an informant is not known
- Existence of FBI foreign intelligence, counterintelligence or international terrorism records are classified fact

**The exemptions most commonly encountered by Navy PAOs in which information may not be released include:**

- A** Properly classified national security information concerning national defense or foreign policy. Proper classifications include Confidential, Secret and Top Secret.
- B** Records that are "related solely to the internal personnel rules and practices of an agency." The tests for withholding under this exemption are:
- The record **MUST** contain personnel-related rules and practices (the word "personnel" should be interpreted as records pertaining to human resources and employee regulations)
  - The records must relate solely to such rules or practices; and
  - The records must be internal to the agency.
- C** Information specifically exempted by a statute establishing particular criteria for withholding, such as:
- Restricted Data and Formerly Restricted Data, 42 U.S.C. 2161–2165 and Atomic Energy Information from Atomic Energy Act of 1954.
  - Communications Intelligence, 18 U.S.C. 798
  - Unclassified Technical Data with Military or Space Application, 10 U.S.C.130.
  - Confidentiality of Medical Records: Qualified Immunity Participants, 10 U.S.C. 1102.
  - Physical Protection of Special Nuclear Material, 10 U.S.C. 128.
  - Procurement Integrity, 41 U.S.C. 423.
- D** Trade secrets and commercial or financial information obtained from a person on a privileged or confidential basis, such as:
- Information contained in loans, bids, contracts or proposals.
  - Statistical data concerning contract performance, income, profits, losses and expenditures.
  - Personal statements in inspections, investigations, or audits that reveal company trade secrets.
- E** Inter- and intra-agency memoranda which are deliberative in nature and are involved in the decision-making process, such as:
- Nonfactual parts of after-action reports and lessons learned containing evaluations, opinions or suggestions.
  - Advice, suggestions or evaluations of consultants, boards, committees, groups or commissions.
  - Speculative information concerning acquiring and disposing of real estate or facilities where release would provide unfair advantage.
  - Trade secret or confidential research or commercial information owned by the government.
  - Information prepared for anticipated administrative or litigation proceedings.
  - Information pertaining to attorney work product or attorney-client privilege.
  - Planning, programming, and budgetary information.
  - Computer software meeting the agency record test.
  - Facts inextricably intertwined with opinions and recommendations.

**F** Information release which constitutes a clearly unwarranted invasion of the personal privacy of other individuals such as that listed below. To withhold the information the privacy interest must outweigh the public interest.

- Employment applications.
- Security clearance records.
- Personnel administrative or disciplinary actions.
- Home addresses and home telephone numbers.
- Personnel and medical files.
- Routinely deployable and overseas units that conduct sensitive operations.
- Social Security Account Numbers

**G** Records or information compiled for law enforcement purposes, but only to the extent that release:

- Could reasonably be expected to interfere with law enforcement proceedings.
- Would deprive a person of a right to a fair trial or impartial adjudication.
- Could reasonably be expected to constitute an unwarranted invasion of the personal privacy of others.
- Could reasonably be expected to disclose the identity of a confidential source.
- Would disclose investigative techniques and procedures.
- Could reasonably be expected to endanger the life or physical safety of any individual.

**H** Names and addresses. Under the Freedom of Information Act (FOIA), a request for names and duty addresses (past, present, and future) of service members attached to units stationed in foreign territories, routinely deployable or sensitive, must be denied under exemption (b)(6) as a clearly unwarranted invasion of personal privacy. Lists of names and duty addresses not covered by this policy may also be exempt under (b)(2) if the administrative burden outweighs any public interest. However, if the requested information is already available in the form requested, such as base telephone directories or organizational charts, it cannot be withheld, as release would not be an administrative burden. Under FOIA, home addresses and telephone numbers are not releasable unless authorized by the service member.

The Navy Freedom of Information Act Office in Washington, D.C., along with their field activities, manages the Navy's FOIA process. Navy FOIA electronic reading rooms are available at [www.foia.navy.mil](http://www.foia.navy.mil) as well as at command and installation websites.

**FOR MORE INFORMATION SEE:**

[www.foia.gov](http://www.foia.gov), Department of Justice Web site on FOIA  
<http://www.dod.mil/pubs/foi/dfoipo/>, DoD's FOIA Web site  
[DoD Directive 5400.7](#), DoD Freedom of Information Act (FOIA) Program  
[DoD 5400.7-R](#), DoD Freedom of Information Act (FOIA) Program  
[www.foia.navy.mil](http://www.foia.navy.mil), U.S. Navy's FOIA Web site  
[SECNAVINST 5720.42F](#), Department of the Navy Freedom of Information Act Program  
[SECNAVINST 5720.44C](#), Department of the Navy Public Affairs Policy and Regulations, Chapter 2

# Privacy Act

While FOIA guarantees the public's right to information regarding government agencies, [the Privacy Act of 1974](#) protects an individual's right to privacy. The Privacy Act was enacted subsequent to the Watergate scandal and in the midst of public concern regarding illegal surveillance and investigation of individuals by federal agencies. It is intended to prevent government agencies from excessive disclosure of personal information maintained by the agency and to grant individuals increased access to agency records maintained on themselves.

Everyone has a constitutional right to privacy including military personnel and government employees. Navy public affairs professionals inherently will have access to significant amounts of personal information on individuals within their organization and must constantly balance the public's right to information with the individual's right to privacy. Such decisions and recommendations must be informed by an understanding of the Privacy Act.

## **Broadly stated, the primary objectives of the Privacy Act as they pertain to public affairs activities include:**

- Restricting government agencies from maintaining personal record systems that are secret or unreported
- Limiting collection of personal information by agencies to those that are relevant and necessary to carry out a purpose mandated by statute or executive order
- Prohibiting the use of personal information collected for one purpose to be used for any other purpose without the consent of the individual
- Mandating agencies to publish notices regarding routine uses of collected personal information and obtaining written consent from individuals for those uses

## **As with the FOIA, the Privacy Act does allow for exceptions to the general rule of “no disclosure without consent” based on the following 12 exemptions:**

- 1 When a transfer of personal information is made within an agency and the receiving office has a bona fide need to know – the Navy and all its components are considered agencies
- 2 When required under FOIA
- 3 When the record or document is used as part of published “routine uses”
- 4 When requisite information is furnished to the U.S. Census Bureau
- 5 For bona fide statistical use in a form in which subjects cannot be identified
- 6 To the National Archives as a historical document
- 7 With the written request of an agency head, to a law enforcement agency and for law enforcement purposes
- 8 In an emergency when personal health or safety is threatened
- 9 To either House of Congress or – to the extent of matters within its jurisdiction – any congressional committee
- 10 To the Comptroller General
- 11 By order of a court from a court of competent jurisdiction (signed by a state or federal court judge)
- 12 To a consumer reporting agency

Generally, the following personal information is releasable and not considered an invasion of personal privacy:

#### For Civilian Employees

- Name
- Present and past grades
- Present and past salaries
- Present and past duty stations
- Office or duty telephone number(s)

#### For Military Service Members

- Name
- Rank and date of rank
- Designator or rating
- Gross salary
- Present and past duty stations
- Future assignments that are officially established
- Office or duty telephone number(s)
- Date and source of commission/enlistment
- Home of record (state only)
- Promotion sequence number
- Awards and decorations
- Attendance at professional military schools
- Duty status at any given time (active, reserve)
- Official photograph

While this information is releasable on a case-by-case basis, blanket requests seeking information on a group of individuals or records should be considered with the help of a Privacy Act expert.

#### WHAT TO WATCH FOR WHEN REVIEWING INFORMATION AND IMAGERY

When reviewing content for release, Navy public affairs professionals ensure that the information or imagery does not contain Privacy Act-protected material. In imagery, look for visible Social Security and other personally identifiable information such as identification cards, building passes, unit rosters, organizational charts, etc. In information watch for information about Sailor's families (including where they reside), date and year married (use how many years the couple has been married instead), names and ages of children and hometowns (use the state only).

#### FOR MORE INFORMATION SEE:

<http://www.justice.gov/opcl/> , Department of Justice Office of Privacy & Civil Liberties  
<http://dpclo.defense.gov/privacy/> , DoD Privacy Web Site  
[DoD Directive 5400.11](#), DoD Privacy Program  
[DoD 5400.11-R](#), DoD Privacy Program  
[www.privacy.navy.mil](http://www.privacy.navy.mil), U.S. Navy Privacy Web Site  
[SECNAVINST 5211.5E](#), Department of the Navy Privacy Program  
[SECNAVINST 5720.44C](#), Department of the Navy Public Affairs Policy and Regulations, Chapter 2

# The Health Insurance Portability and Accountability Act (HIPAA)

The unauthorized release of Protected Health Information (PHI) is a crime. To safeguard PHI, military treatment facilities have implemented the HIPAA policies contained in the DoD Health Information Privacy Regulation, which prohibits the release of information unless allowed by the patient or by specific exception.

PHI is individually identifiable health information of an individual, relating to past, present or future medical conditions and transmitted in any form (including orally, on paper or electronically).

**The elements of PHI which apply to personnel operating under HIPAA include, but are not limited to:**

- Name.
- Address.
- Date/s of care.
- Date of birth.
- Social Security number.
- Facial images.
- Details of the medical condition or care provided.

DoD has developed two forms in support of HIPAA. The first, [DD Form 2870](#), authorizes the disclosure of medical or dental information by a patient. The second, [DD Form 2871](#), an individual may use to restrict the release of medical or dental information.

A signed, HIPAA-compliant consent form (DD Form 2870) from the patient is required to disclose PHI. Even with such consent, a reasonable effort must be made to limit the use, disclosure or request of PHI to the minimum necessary to accomplish the intended purpose.

Unless the patient objects or requests that his PHI be restricted, Navy public affairs professionals may release the patient's one-word condition to individuals who inquire about the patient by name without obtaining prior patient authorization. A patient's room number may not be given to the media without the patient's authorization. A general location such as intensive care unit, burn unit, etc., is permitted.

**Only medical professionals are authorized to determine the condition description as one of the following:**

- Undetermined
- Good
- Fair
- Serious
- Critical

The covered entities required to comply with HIPAA are defined by the Assistant Secretary of Defense (Health Affairs) as a health care provider, health plan, or health care clearinghouse who transmit any health information in electronic form. In general, that applies to all health care personnel, hospitals, medical clinics, dental treatment facilities, labs and billing agencies. HIPAA regulations do not apply to authorized DoD drug testing programs, the Armed Forces Repository of Specimen Samples for the Identification of Remains, reserve component medical activities that are not practicing in a military treatment facility, or Military Entrance Processing Stations, nor do they apply to the provision of healthcare to foreign national beneficiaries of the military health system when such care is provided in a country other than the United States.

HIPAA applies only to information gathered by those acting on behalf of the entities listed above. Those who are not acting on behalf of the listed entities may release information that is available by other means, such as a service record or other official documentation, provided that release complies with the provisions of the Privacy Act.

Both the Privacy Act and HIPAA establish exceptions to the release of PHI under FOIA, especially when it would cause unwarranted invasion of privacy.

**Authorizations for release of information should be completed using a DD Form 2870; however, if this form is not available, the following must be included:**

- A description of the information to be used or disclosed in a specific and meaningful fashion.
- The name or specific identification of the person(s).
- The name or specific identification of the person(s) to whom the covered entity may make the disclosure.
- A description of the purpose of the disclosure.
- An expiration date or event that relates to the individual or purpose of the disclosure.
- Signature of the individual and the date.
- A statement the individual has the right to revoke the authorization in writing.
- A statement on the ability or inability to make authorization a condition of treatment, payment, enrollment or eligibility benefits.
- A statement indicating the potential for the information being disclosed pursuant to the authorization to be subject to re-disclosure by the recipient and no longer protected by HIPAA.
- The individual will be provided a signed copy of the signed authorization.

#### WHAT TO WATCH FOR WHEN REVIEWING INFORMATION AND IMAGERY

In general, the same HIPAA rules apply when reviewing imagery. When reviewing content for release, Navy public affairs professionals should consult with the Staff Judge Advocate and the military treatment facility privacy officer as quickly as possible to ensure applicable requirements are met in each circumstance. Additionally, they must ensure that the information or imagery does not contain PHI and that patients are not identifiable unless the patient featured has signed a release authorizing the release of PHI or identifying him.

## Without consent

If requested by name, the patient's one-word condition (undetermined, good, fair, serious, critical)

Exterior shots of facility

Interior shots of equipment and spaces

Visuals of military treatment facility personnel at work that do not include any image that would identify a patient

Imagery showing back and back ¾ view of a patient as long as positive identification cannot be made

Imagery showing patient medical records as long as no PHI is visible

Imagery showing medications/prescription bottles as long as no PHI is visible

## With Consent

Images of patients' faces where positive identification can be made

Patient's medical records  
(Images may be permitted if no PHI is visible)

Hospital identification bracelets  
(Images may be permitted if no PHI is visible)

Interaction with minors

Distribution lists and directories with patient locations

Medications showing patient names and information, such as a prescription bottle

Ranks or statements suggesting identity, such as "admiral," or "flag officer," etc.

### FOR MORE INFORMATION SEE:

[DoD 6025.18-R](#), DoD Health Information Privacy Regulation  
[SECNAVINST 5720.44C](#), Department of the Navy Public Affairs Policy and Regulations, Chapter 2  
[DD Form 2870](#), Authorization for Disclosure of Medical or Dental Information  
[DD Form 2871](#), Request to Restrict Medical or Dental Information

# Copyright

Intellectual property is defined as intangible products of the mind or intellect regardless of the medium through which they are conveyed. Copyright laws safeguard the right of the original creator of a particular work to control and profit from the production of his or her work, while trademark laws protect the words, names, and symbols used by organizations to identify and distinguish themselves among others.

The Copyright Law of the United States, contained in [Title 17, U.S.C.](#), prohibits the reproduction, distribution, adaptation, performance, or display of copyrighted material without the copyright owner's permission. However, copyright laws do not pertain to facts, events, ideas, plans, methods, systems or blank forms. With the enactment of the [1998 Digital Millennium Copyright Act](#), copyright protection expands to cover digital material regardless of the format or medium. The eight categories of copyrighted materials are:

- 
- literary works
  - musical works, including any accompanying words
  - dramatic works, including any accompanying music
  - pantomimes and choreographic works
  - pictorial, graphic, and sculptural works
  - motion pictures and other audiovisual works
  - sound recordings
  - architectural works

The Department of Defense and the Navy recognize copyright ownership. It is policy not to incorporate work that would infringe on a copyright. If an infringement occurs, and it goes to court, the owner's only recourse is against the government. Action will be taken if infringement was done either deliberately or through negligence.

Material is considered in the public domain when the copyright of a work has expired or the creator of the material never claimed copyright. Furthermore, intellectual property is subject to public ownership when the material is produced by federal employees in their official capacity or using federally-owned equipment such as computers. This directly applies to content developed by Navy public affairs professionals in the execution of their duties, placing all official Navy content in the public domain.

However, works created by federal employees off-duty using equipment they own may be copyrighted. Uniformed or civilian Navy personnel creating works based on their Navy experiences should contact their legal office for additional guidance on potential ethics rules violations. Uniformed or civilian Navy personnel authoring books should work with the Navy Office of Information East in New York City to obtain the necessary clearances.

## WHAT TO WATCH FOR WHEN REVIEWING INFORMATION AND IMAGERY

When reviewing content for release, Navy public affairs professionals ensure that the information or imagery does not contain copyrighted material. This issue comes up most frequently with videos, either with the video set to a copyrighted song or a video containing copyrighted clip. When reviewing information and imagery, be sure to ask the content creator where article excerpts, background music and video clips used in the product were sourced and ensure the source material actually used does not have a copyright or that the command has permission from the copyright holder to use the material. Permission must be in written form and remain in command files.

### Sources of Music for Use In Videos Created for Public Release

#### Killer Tracks

CHINFO has U.S. Navy Public Affairs (PA) annual enterprise license with Killer Tracks (KT), a Los Angeles-based company. This license allows a U.S. Navy ship or station in the U.S., its territories and at overseas military installations to access a comprehensive library of music tracks available on-line in multiple file formats. KT has 21 libraries showcasing thousands of tracks cataloged by a growing list of classical and contemporary genera. Navy Media Content Services (OI-2) has four portable hard drives each containing all 21 collections. OI-2 will ensure future deployed carrier media departments have this content locally aboard ship in time for major deployments. Email [NavyMedia@navy.mil](mailto:NavyMedia@navy.mil) to receive business rules and information for log-in and password.

#### Navy Bands

If you are preparing a production and don't want to go through the approval process or don't have the time to do so you could contact the nearest Navy Band and request its CDs. These recorded performances of popular and military themed music are perfectly acceptable for producing local, one time, multimedia productions.

#### Copyrighted Music

Consent to use copyrighted material can be costly, dependent on the value of the material. The original creator of the copyrighted work is often not the owner of the copyright. The copyright owner will often grant the military services permission to make limited use of the material without a charge. Unless you know there will be a fee, make your initial request for free permission.

## Requesting permission to use copyrighted material

SECNAVINST 5870.4A requires permission to be requested directly from the copyright owner or the owner's agent. Include the following in your request:

- Complete identification of the material, including the title of the program, name of author or artist, exact copyright notice(s) appearing on the work, and when appropriate, date and time of airing
- Designation of the exact portion of the work to be used (e.g. amount, time, segments). Requests for blanket permission to use excerpts "as later determined" are not acceptable
- Statement of intended use(s) of the material including, when appropriate, number of copies to be made; intended distribution, whether material is to be sold and contemplated fees or charges in connection with use or distribution of the materials; length of time material will be used; and dates, media, and intended audience of public performances or displays
- Intended modifications of the work, if any

Do not request greater rights than are actually needed. Submit your request in duplicate so the recipient may retain one copy and return the other granting permission. Indicate on your request that the copyright owner may designate the copyright notice and credit line to be used. Enclose a self-addressed return envelope.

If approval is granted, a copy of the approval must be maintained with the work request until the work request is destroyed, and then it should be filed indefinitely.

### FOR MORE INFORMATION SEE:

<http://www.copyright.gov/>, U.S. Copyright Office  
[DoD Directive 5535.4](#), Copyrighted Song and Video Recordings  
[SECNAVINST 5870.4A](#), Copyright  
[SECNAVINST 5720.44C](#), Department of the Navy Public Affairs Policy and Regulations, Chapter 2

# Defamation

Aside from laws relating to privacy and access to information, Navy public affairs professionals must be versed in other communication laws, including those pertaining to defamation. Essentially, defamation deals with the dissemination of false information that damages the reputation or standing of an individual, while privacy laws involve factual information. Defamation is categorized as either slander, which is spoken or verbal defamation regardless of public setting, and libel, which is published or broadcast information. Libel is traditionally considered a more serious offense, considering the inherent characteristics of published or broadcast communications. Libel implies permanent, widespread, and intentional damage, as information broadcast through television, radio, or the Internet becomes an enduring part of the public record with vast, uncontrolled exposure. Further, the act of composing, editing, and disseminating defamatory information presumes a pre-planned intent to falsely communicate information regarding an individual.

Navy public affairs professionals must avoid engaging in communication that might be defamatory, whether libelous or slanderous. While no federal laws exist that pertain to libel, the majority of state laws require five key elements to be present for information to be considered legally libel:

- It was published or broadcast
- It identified someone unfavorably
- It was created by a person that was negligent or reckless
- It was stated as a fact even though it was false
- It caused injury to the person identified

Any individual, business, nonprofit group, or association has the right to pursue libel charges, however government agencies cannot sue for libel as the right to criticize government activities is an inherent right of citizenry under the First Amendment. Still, an individual within the Navy who believes he or she has been libeled or slandered concerning the performance of official duties may institute legal action.

## WHAT TO WATCH FOR WHEN REVIEWING INFORMATION AND IMAGERY

When reviewing content for release, Navy public affairs professionals ensure that the information or imagery does not defame the organizations and individuals depicted. The following general guidelines can help prevent accusations of defamation:

- Attribute sources and establish policy on the use of the word “alleged”
- Only accuse someone of a crime if there is a confession, accusation or conviction by an official legal body – remember that accusations of a crime must be supported with criminal reports from official sources
- Avoid attributing physical or mental disease to an individual – remember, the Privacy Act and HIPAA protect medical records
- Do not associate a person with a group or cause that is held in disrepute
- Do not accuse someone of poor moral character
- Do not accuse someone of being incompetent or dishonest in his or her profession
- Avoid sexist, racial or ethnic slurs

# Considerations Unique to Imagery

Common sense and good taste are the keynotes of imagery for public release. Most of the following guidelines come from DoD directives and apply across the board but there are exceptions to each.

## APPEARANCE

Show Navy personnel properly clothed and equipped. Military members' personal appearance must conform to standards whether on or off the installation.

## INSTALLATIONS

Unclassified photographs of installations must meet directives that apply on releasing unclassified information, including security review requirements.

## COURTROOMS

No photographs will be taken of open or closed court sessions. A photo of the accused with an ID frame may be requested through the FOIA.

## MERCHANDISE ENDORSEMENTS

Do not photograph Navy personnel with products or merchandise with trade names appearing in such a way that it implies Navy endorsement.

## SIGNS AND POSTERS

Don't photograph them if they are in bad or poor taste.

## SUGGESTIVE PHOTOGRAPHS

Do not take obscene or suggestive photographs. Avoid pin-up, or suggestive photographs of Navy personnel, and do not concentrate on any one individual because of his/her appearance.

# Considerations Unique to Visual Information Productions

The DoD and the Navy must avoid liability under laws that protect persons and their property from invasion of privacy, trespass, and violation of rights in property. All productions produced for the Navy and intended for public release shall undergo a legal review to establish legal clearances, restrictions, or conditions. This review shall be conducted by a judge advocate or other legal counsel in coordination with the production activity. The record of legal review shall become a permanent part of the official production folder.

## Activities that create productions shall obtain signed releases from the following persons:

- Persons who either appear in, or whose voices are used in, a production.
- Persons whose minor children, real estate, or other private property appears, in any production

## To determine the need for releases, apply the following guidelines:

- No release is required from active duty military personnel including cadets or midshipmen of the U.S. Military Academies or DoD civilians performing their official duties.
- Under most circumstances, an individual's expectation of privacy changes with the situation. Releases should be obtained from persons depicted in commonplace, secluded, or in unspectacular situations. Newsworthy or public events provide little, if any, expectation of privacy and do not require releases.
- If an individual is part of a crowd, no release is required. When an individual is a central figure in a scene, a release is required regardless of the brevity of the scene.
- Copyrighted material always requires separate clearances. Follow the guidelines provided in the Copyright section.

## FOR MORE INFORMATION SEE:

[DoD Instruction 5040.07](#), Visual Information (VI) Production Procedures

# Investigations Accused Individuals

## Considerations

In military justice matters, the Navy must balance individual rights, the public interest and the best interests of the Navy, in that order. Judicial matters are of frequent interest to the public. However, unauthorized disclosure of details on a matter under investigation or referred to court martial may violate the rights of the accused, hamper the government's case, unduly influence the litigation process or violate the Department of Justice guidelines on trial publicity.

## Coordination

Consult with the appropriate investigating officer or organization (NCIS, Navy Inspector General) prior to releasing information on investigations. Consult with the staff or command judge advocate and defense counsel before releasing information on non-judicial punishment, courts martial or to obtain the current region docket. JAGINST 5800.7F pertains.

Refer requests for interviews with the accused to defense counsel. In general, news media representatives may attend open sessions of courts martial. Matters with potential for national or international media interest will be submitted through the chain of command to OASD(PA).

## Releasable

- Non-Judicial Punishment (NJP)
- General information such as rank, offense and disposition in base papers, plan of the day and response to query only
- Court Martial
- Prior to charges being preferred, may release that an investigation is in progress and no charges have been filed
- Once charges are preferred and referred to a General or Special courts martial, the following may be released upon request:
  - Name, grade, age, unit duty station and gender
  - The offense that the individual has been charged with, with a statement that the charge is merely an accusation and the accused is presumed innocent
  - Identity of the apprehending and investigating agency
  - Identity of the accused's counsel, if any
  - The time and place of apprehension of the accused and the nature of any pre-trial restraint imposed
  - The result of any stage in the judicial process
  - Charge sheets if redacted of private or privileged information

- Docket. Dockets should be made available to the public and may include the following:
  - Grade and service of the accused
  - Time, date and place of the proceedings of Article 32, UCMJ, investigations and courts-martial hearings
  - General nature of the proceeding (arraignment, motions, trial)
  - General nature of the offense(s)  
(for example, Article 86 – Absence without leave)

## Not Releasable

- Information that would violate security
- Potentially influential or compromising information on an investigation in progress
- No imagery (photo/video) of the accused before he/she is advised of his/her rights; then choice is the accused's
- Information on NJP or other administrative proceedings unless particularly newsworthy (e.g. senior official or major issue)
- Civil criminal investigatory matters
- Avoid editorial words prejudicial to the accused such as “criminal”
- Safety and occupational safety and health inspections
- Investigation content that violates the Navy's agreement with sources
- Investigation content that could undermine future investigations

# Criminal Activities and Arrests

## Considerations

Occasionally, Navy personnel (either military or civilian) will engage in criminal activities and be arrested. When individuals are arrested off-base, civilian law enforcement agencies have jurisdiction and the matter becomes part of the public record – that is, the information is in the public domain. When individuals are arrested on a Navy installation, the matter does not become part of the public record until a public release is made by Public Affairs. Such releases should focus on the facts.

## Coordination

If the activity occurred on a Navy installation, Naval Criminal Investigative Service (NCIS) will investigate and any releases must be coordinated with them. If the criminal activity occurred within the jurisdiction of civil authorities, then the lead civilian organization will be the release authority.

## Releasable

- Names, grades, ages and units of those involved (Next of Kin notification requirements do not apply if there are no deaths or injuries; names of family members generally cannot be released)
- Location and time of event(s)
- Command response

## Not Releasable

- Names of the family members of those engaged in the criminal activity or arrested.

# Prisoners of War (POWs) U.S. Forces

## Considerations

In spite of the presence of news media in conflict areas, the public may not have immediate knowledge of a service member's capture. Permitting the next of kin notification process to work is paramount. After that process is complete and 24 hours have passed, unless there is a bona fide OPSEC reason to withhold release, information will be publically released by DoD.

## Coordination

The initial release will be made by DoD or the designated authority. The Navy will respond to further queries for personal information concerning Navy POWs when directed by DoD.

## Likely Messages

- The U.S. expects members of the Armed Forces who are POWs to be treated in accordance with the Geneva Conventions (including prohibitions against torture and food deprivation)
- All military members receive training on the U.S. Code of Conduct, a moral guide that helps military personnel abide by the Geneva Conventions and to survive and return with honor.

## Releasable

- By DoD in the initial release
  - Name • Rank • Assigned unit • Age
  - Confirmation that the service member is a POW
- By the Navy in a secondary release once directed by DoD:
  - Home of record (state only)
  - Official photo (if on file)

## Not Releasable

- Individually identifiable health information
- Information concerning the activities the service member was engaged in when captured and the circumstances of the capture (for OPSEC)

# Prisoners Under Control (PUC) Enemy Prisoners of War (EPWs)

## Considerations

The need to provide accurate and timely information to the public regarding Persons Under Control, Civilian Internees and Enemy Prisoners of War must be weighed against the need for operations security and personal privacy. Additionally, the provisions of the Third Geneva Convention of 1949 must be met for EPWs.

## Coordination

Interviews and photography/videography of PUCs must be coordinated in advance with the Staff Judge Advocate, Legal Advisor's Office or higher authority to ensure compliance with the Law of Armed Conflict and, in the case of EPWs, compliance with requirements of the Third Geneva Convention of 1949.

Prior to allowing coverage of enemy prisoners, PAOs must discuss the limitations of media coverage with news media representatives to include requests for post-coverage review of photos, video or any other products.

## Releasable

- Interviews with commanders, support staff, medical professionals and detention camp personnel are permitted and encouraged as they may be an appropriate way to illustrate the humane treatment of enemy prisoners

## Not Releasable

- Imagery of EPWs limited in accordance with protections provided by the Third Geneva Convention of 1949; not releasable until authorized by DoD or a delegated authority.
- Any coverage that would reveal the identity of an individual EPW

# Counter Narcotics Operations

## Considerations

Counter narcotics operations are inherently sensitive and involve a number of risks which may be heightened by the release of information to the public. These risks only can be minimized through comprehensive coordination BEFORE any information is released to the public.

## Coordination

DoD counter narcotics operations are never unilateral and always require coordination with either civilian law enforcement, the U.S. Coast Guard, other Services or DoD agencies, or host nation military, police or security forces. All news releases must be coordinated with the lead agency (usually Coast Guard, FBI or DEA) AND with the command judge advocate.

## Likely Messages

- Cooperation with civilian agencies
- Flexibility
- National security interests
- Jointness

## Releasable

- Previously approved statements and associated messages and RTQs pertaining to the Navy's role in support of counter-drug operations that make the appropriate differentiation with the law enforcement aspect of the operation.
- Copies of DoD-originated speeches and printed materials already in the public domain

## Not Releasable

- Any information and imagery not coordinated with the lead agency including:
  - Names of participating military and civilian personnel
  - Sources of intelligence
  - Intelligence-gathering procedures

# Base Realignment and Closure (BRAC)

## Considerations

Base Realignments and Closures (BRAC) are contentious and controversial issues. Each time a BRAC process is enacted, DoD will provide specific PAG on that process. All commanders and their PA representatives will become familiar with the PAG and will adhere to it. Supplemental PAG may be issued within DON. Commanders and their public affairs representatives must be prepared to respond to questions and objectively communicate the details of the BRAC process to the public.

## Coordination

Navy instructions outline the coordination and clearance requirements for information dealing with base closures, force reductions and other actions with significant social or economic impact. Because major changes in the status of activities normally result in intense Congressional and public interest, all actions must be examined, planned and coordinated at the highest levels so that the integrity of those decisions can be demonstrated to Congress and the public. The timing and nature of information released may require careful attention to conform to the environmental impact statement process. The following requirements are germane:

- In no case should there be any public confirmation or discussion of an action with significant social or economic impact until coordination has been completed at the proper level of government. The following statement should be used in case of media query concerning closure, reduction, increase, establishment, consolidation or other action:  
“The status of all Navy installations and operations are constantly being reviewed in light of operational requirements and budget priorities. This review is part of an ongoing study to bring about increased efficiency and combat readiness while reducing costs. When decisions are made, Congress and the news media will be informed.”
- The office, command, fleet or systems command with primary cognizance over the matter is responsible for preparing a fact sheet, news release and contingency responses to query and any public affairs guidance to CHINFO, which will coordinate the public release of information when necessary.
- After coordination with appropriate authorities and before public release, the Chief of Legislative Affairs will inform interested members and committees of Congress.
- Notification of local authorities: State officials and local news media will be notified by cognizant Navy commands as soon as possible after congressional notification and preferably simultaneous with release to national news media.

## Releasable

- The types of information normally provided, as long as an overriding requirement of a BRAC commission does not otherwise prohibit such release. The typical information includes, but is not limited to:
  - Command mission
  - Installation economic impact
  - Approximate number of employees.

## Not Releasable

- Information, in whole or part, contained in data calls or other responses to BRAC officials
- Answer questions requiring speculation and/or discussion of BRAC issues that are subject to internal DoD deliberation

# Scientific and Technical Information (STI)

## Considerations

Scientific and technical information (STI) is increasingly important in today's high-tech world and technologically advancing Navy and provides a warfighting advantage over our adversaries. Accordingly, STI frequently is sensitive. The Navy's Scientific and Technical Information Program exists to improve the processing, dissemination, application and retention of Navy STI. The program ensures STI generated by research, development, test and evaluation (RDT&E) is used to advance Navy, Department of Defense and national RDT&E efforts.

## Coordination

The public affairs offices at the Office of Naval Research and the Naval Research Lab can assist with questions on the release of STI information.

## Releasable

- Contact ONR or NRL for specifics as to what can be released or not released.

## Not Releasable

- Contact ONR or NRL for specifics as to what can be released or not released.

# Congressional Inquiries

## Considerations

Media queries often parallel the concerns and interests of members of Congress, thus it is critical that PA professionals understand the congressional issues that drive media interest, as well as the extent of media influence on government officials and their constituents.

## Coordination

On inquiries with international, national or DON-wide interest, consult with the Office of Legislative Affairs. For guidance on the security review of information before releasing it to Congress, see OPNAVINST 5510.158A, "Security Review Guide for Congressional Matters."

On inquiries regarding individuals within your command, work with your N1 and Legal Office. Commands and offices may disclose information about individuals within their jurisdiction to either house of Congress or to any committee or subcommittee of Congress, if they have a written Privacy Act release signed by the individual. Commands may not disclose protected personal information to a Member of Congress without a signed written Privacy Act release under any circumstance.

## Releasable

- If the receiving command is in routine contact with a state's Congressional delegation AND if the information requested is of a routine nature of negligible national or DON-wide impact, the command may respond without referral to a higher authority. Examples:
  - Obtaining surplus military material for a local installation.
  - Requesting an organized tour for a group civic leaders
  - Requesting information on how to apply for civilian positions at the command.
- Commands and offices may disclose information about individuals within their jurisdiction to either house of Congress or to any committee or subcommittee of Congress, if they have a written Privacy Act release signed by the individual.

## Not Releasable

- Commands may not disclose protected personal information to a Member of Congress without a signed written Privacy Act release under any circumstance.