

美國涉密聯邦政府員工之機密資訊維護-保密協議（Non-disclosure Agreement, NDA）之使用



美國涉密聯邦政府員工之機密資訊維護-保密協議（Non-disclosure Agreement, NDA）之使用

科技法律研究所
2013年12月06日

壹、事件摘要

前美國海軍海豹部隊（SEAL）隊員Matt Bissonette以化名Mark Owen出版 *No Easy Day* 一書，內容主要描述狙殺Osama Bin Laden的規劃與執行，並蟬聯最佳暢銷書籍。美國國防部對Matt Bissonette提出洩露國家機密之訴訟，及違反保密協議的規定。以下簡介美國對於聯邦政府官員的機密維護規範及措施，包括保密協議之使用、違反保密協議時對於該聯邦政府員工的追訴以及對於未經授權被揭露之機密資訊的防護；更進一步，聚焦探討美國以「保密協議」規範聯邦政府員工的方式，提供我國參考。

貳、重點說明

一、總統行政命令與機密資訊維護

傳統上，美國對於機密資訊由軍事單位依照軍事規定處理，不過，自從羅斯福總統於1940年發布第8381號行政命令，改變了這個機制。總統第8381號行政命令，授權政府官員保護軍事與海軍基地；爾後，歷任總統便以發布行政命令的方式，建置聯邦政府的機密分級標準，以及各項為維護國家安全的各項法令規定與措施。不過，羅斯福總統係以經特定法規授權為由而發佈總統行政命令，羅斯福以後的總統則是基於一般法律與憲法授權[1]，為維護國家安全之憲法上的責任而發佈總統行政命令；於此，國會則不停的以其他立法的方式，設法平衡總統行政權與國會立法權間權利[2]。

有關總統行政命令之效力，如其規範的主題相同時，新的行政命令效力將會取代前案行政命令。目前美國政府有關機密係根據歐巴馬總統於2009年所發佈總統第13526號行政命令，主題為「國家安全機密資訊（Classified National Security Information）」，其內容及效力取代前行政命令，修改美國聯邦法規第32章2001篇涉及國家安全之機密資訊（32 C.F.R. 2001 Classified National Security Information）[3]，以及勾勒機密資訊分級、解密、機密資訊的處理等議題的框架。

二、涉及國家安全機密資訊之安全維護措施

依據總統第12958號行政命令，機關必須採取管控措施保護機密資訊，包括使用（Access）機密資訊的一般限制、分布機密資訊的控制，與使用機密資訊的特別計畫。第12958號行政命令Sec.4.2（a）規定使用機密資訊的一般限制[4]：聯邦政府員工使用機密資訊前，必需符合下列三大前提要件，包括通過「人員安全檢查（Personnel Security Investigation）」、簽署「保密協議」，與執行職務所「必要知悉（Need-to-know）」，才得以使用機密資訊[5]。

第一項前提要件為「人員安全檢查」，其安全檢查目的在於確定使用機密資訊人員的可信賴度（Trustworthiness），在相關部門或機構完成安全調查確認該人員的可信賴度之後，將授予通過安全檢查的資格，進而進入第二步驟「SF312保密協議」的簽署[6]。

第二項前提要件為簽署「保密協議」，係由美國總統指令所要求，並於總統行政命令所重申[7]凡涉及使用機密資訊之聯邦政府員工（Employee of the Federal Government）、承包商（Contractor）、授權人或受讓人（Licensees or Grantees）等，於使用機密資訊前，必須完成「保密協議」的簽署，否則不得使用。該「保密協議」在法律上為拘束簽署員工（前述通過安全檢查之人員）與美國政府間的契約

(Contract) [8]，簽署員工承諾，非經授權不得向未經授權之人揭露機密資訊[9]。

「保密協議」的主要目的在於「告知 (Informed)」簽署員工：

1. 因信任該員工而提供其使用機密資訊；
2. 簽署員工保護機密資訊不得未經授權揭露的責任；與
3. 未能遵循協議條款後果。

第三項要件係說明政府聯邦員工得使用機密資訊的範圍，以該員工執行職務所「必要知悉 (Need-to-know)」為限。

三、保密協議

「保密協議」(Classified Information Non-disclosure Agreement，一般簡稱為NDA)為機密資訊安全維護措施之一，美國政府藉由該契約協議的內容條款，確立信任關係、責任的範圍，以及未遵循契約條款的後果，並得以此協議防止簽署人未經授權揭露機密資訊，或簽署人有違反情事，對其提起民事或行政訴訟[10]。

通過安全查核者 (Security Clearance)，將被授與特權 (Privilege)，此權限不是與生俱來的權利 (Right)。當獲得使用機密資訊的特權時，使用人必須背負相對的責任。簽署人一旦簽署與美國政府之間具法律拘束力的「保密協議」，即表示同意遵守保護機密資訊的程序，並於違反協議條款時，受到相對的處罰[11]。

美國利用「保密協議」約束員工對於機密資訊的保護，要求員工於發佈資訊之前，必須將內容提交機構進行審查。著名的案子為Snepp v. United States，最高法院對於「中央情報局 (Central Intelligence Agency, CIA)」的前情報員，強制執行所簽署的保密協議，因前員工未遵守與中央情報局間的協議條款，亦即於出版書籍之前，先行提交出版內容給中央情報局審查的約定，中央情報局進而對該書籍的利潤施以法定信託 (Constructive Trust)，即使中央情報局最終的判斷內容未含機密資訊[12]，也不影響該決定的效力。

(一) 「保密協議」的法源基礎

在數個與國家安全機密資訊相關的總統行政命令中，現行「保密協議」所依據法源為總統第12958號行政命令。第12958號行政命令規定，由「資訊安全監督局」(Information Security Oversight Office, ISOO)負責監督行政部門與政府機關對於「涉及國家安全之機密資訊」的創建或處理事宜[13]。

資訊安全監督局局長為遂行涉及國家安全機密資訊之維護，於1983年頒佈「國家安全決策第84號指令」(National Security Decision Directive No. 84, NSDD 84) [14]規範進行國家安全機密資訊之維護。雖然「保密協議」曾經被挑戰，但卻一直受到聯邦法院 (包括最高法院) 的支持，為具有法律拘束力和合憲性的文件[15]。

「國家安全決策第84號指令」規定，凡通過安全檢查之人員[16]，必須完成簽署制式保密協議，並待生效後，才得以使用機密資訊。換句話說，相關人員必須以有效的保密協議為條件，才得以使用機密資訊。

「保密協議」應經過「國家安全委員會 (National Security Council)」批准，與「司法部 (Department of Justice)」的審查，而為法院可執行，而且機關不得接受經簽署員工單方修改用語的「保密協議」[17]。

目前「保密協議」版本稱為312制式表格 (Standard Form 312)，以下簡稱「SF312保密協議」[18]。

(二) 「SF312保密協議」關於 (Classified Information) 的定義[19]

「SF312保密協議」的「機密」係指標示或未經標示的機密資訊，包括非書面的口述機密資訊，以及雖未歸屬於機密資訊但符合第12958號總統行政命令Sec. 1.2或1.4 (e)的規定[20]，符合機密資訊的標準，或依據其他總統行政命令或法規是否為機密的確認期間 (Pending) 先行提供機密資訊保護的資訊；但並不包含在將來可能會被歸屬於機密，但目前尚未進入機密分級過程中的資訊[21]。

歐巴馬政府有關國家機密資訊之第13526號行政命令[22]，於機密資訊安全維護部分之內容，仍與第12958號總統行政命令相同[23]。得使用機密資訊之人員僅限向相關主管機關首長展現其使用的資格，並簽署保密協議者，且限於其職務所必要知悉的範圍內，使用機密資訊。

(三) 違反「SF312保密協議」的責任[24]

若「SF312保密協議」的簽署員工「知悉或應合理知悉 (Knows or Reasonably Should Know)」，該資訊為已標示或未經標示的機密資訊，抑或符合機密資訊的標準但仍處於確認過程的資訊，而其行為將導致或於合理情形下可能導致未經授權揭露機密資訊，則可能需負未經授權揭露機密資訊的法律責任。因此，如於揭露資訊的當時，無根據可認定該資訊為機密資訊或可能成為機密資訊時，該簽署員工不會因為揭露該資訊，而需負未經授權揭露機密資訊的責任[25]。

另外，直至正式解密 (Officially Declassified)，機密資訊不因已被揭露於公共來源 (Public Source)，例如大眾媒體，而解密。不過，如僅於公共來源以抽象的方式引述該筆機密資訊，並非屬於再度未經授權揭露機密資訊[26]。

「SF312保密協議」簽署員工於資訊傳遞前，或確認公共來源資訊的正確性時，需先行向有權機關確認該資訊已被解密；若該員工未進一步履行確認資訊機密性，而逕進行資訊傳遞或確認資訊正確性時，該行為將成屬於未經授權揭露機密資訊[27]。

(四) 「SF312保密協議」的有效期間

「SF312保密協議」載明，保密協議對於簽署員工的拘束力，從被授權使用機密資訊之時點開始，該員工終身均負保密義務[28]。

該條款明白表示，國家安全敏感性相關的機密資訊，與任一特定個人安全檢查資格的有效期間，並不相關。易言之，未經授權揭露機密資訊對美國所造成的傷害，並不取決揭露人的身分而有不同[29]。

是以，實務上，機關多以違反「保密協議」為訴因，對退職或離職之員工，進行民事或行政訴訟。

「SF312保密協議」所規範的保密義務，適用於所有機密資訊，然而，若某特定資訊已經解密，則按照「SF312保密協議」的規定，該簽署員工則不具持續保密的義務。此外，該「SF312保密協議」的簽署員工，還得發動強制性審查的請求，尋求解除特定的資訊的密等，包括該簽署員工

具有使用權限的機密資訊[30]。

(五) 違反「SF312保密協議」美國政府可採取的行動

聯邦政府員工如有明知、故意或因過失而未經授權揭露機密資訊，或任何合理預期可能導致未經授權揭露機密資訊之情事，機關首長或資深官員必須即刻通知資訊安全監督局，並採取「適當和及時的校正行動」[31]。

基於「SF312保密協議」，對於未經授權揭露機密資訊事件，美國政府可能至美國聯邦法院提起民事與行政訴訟。

民事訴訟可能分為禁制令（Injunction）、民事金錢損害賠償，與所得利益的追討。

1. 禁制令

請求聯邦法院申請發佈禁制令，以禁止公布與以其他方式揭露該機密資訊。例如 *United States v. Marchetti* 案，聯邦法院發佈禁制令，防止前中央情報局情報員以出版書籍的方式揭露機密資訊[32]；或是國務院以撤銷護照的方式，管制人員出境（儘管該人員出國的目的為暴露秘密情報員的身分，擾亂情報工作，而非協助他國政府）[33]。

2. 金錢損害賠償

向該員工請求美國政府因未經授權揭露機密資訊所造成損失之金錢的損害賠償。

3. 所得利益之追討

償還美國政府因未經授權揭露機密資訊所得之相對代價，或其他金錢或財產上的所得[34]。

如「SF312保密協議」簽署員工違反協議，則美國政府可對其進行行政裁處與處罰，包括譴責（Reprimand）、暫時吊銷（Suspension）聯邦政府員工資格、降級（Demotion），或甚至撤職（Removal），並可能被取消通過安全檢查的資格[35]。

雖然，聯邦政府員工於違反「SF312保密協議」時，美國政府得以違反契約（SF312保密協議）為訴因，向簽署員工提起民事或行政訴訟；不過，如果該員工的行為亦已違反其他刑事規定，政府也可能同時對該洩密員工提起刑事訴訟[36]。但是，法制上並不存在總括性（Blanket Prohibition）規定，處罰所有未經授權揭露涉及國家機密資訊的處罰[37]。

例如，機關得依據 18 U.S.C. §798 揭露機密資訊（Disclosure of Classified Information）提起刑事訴訟，美國政府必須設法證明符合該條文的構成要件之故意，與該當法條所規定揭露機密資訊要件之狀況。該刑事的舉證責任，比起違反保密協議的舉證責任重了許多；不過，相對的，如政府可舉證證明，其處罰也會比違反保密協議重了許多，不是只有因洩密行為而獲得的利益被沒收，法院還得處以監禁（Incarceration）與罰金（Fines）[38]。

參、事件評析

美國規範認定，使用機密資訊的權限為被授與的特權，而不是與生俱來的權利。美國聯邦政府利用與員工之間的雇用關係，透過保密協議（契約關係）的方式，規範該政府員工對於機密資訊的維護，載明雙方的關係、政府員工的保密責任，以及違反保密協議的後果，並強調該保密協議的效力，一直持續至該員工的終身，這意味著，政府員工於不具安全檢查的資格之後，或甚至是退離職之後，仍受保密協議的拘束。

除了對於員工本身的權利義務與罰則加以規範之外，美國政府亦特別著重於資訊的快速擴散性與保持機密性的需求，對於未經授權而揭露的機密資訊，利用違反保密協議（違約）（Breach of Contract）為手段，儘量減少機密資訊擴散的程度。例如，美國政府對政府員工提起告訴時，以舉證責任來看，證明違反保密協議民事的舉證責任，比需要證明行為人違反刑法規定的刑事舉證責任為輕。再者，透過禁制令的方式，凍結並維持資訊的「現有狀態（Status Quo）」，並且還得於提起民事訴訟的同時，提起刑事。

[1] Jennifer K. Elsea, *The Protection of Classified Information: The Legal Framework* (2013) CONGRESSIONAL RESEARCH SERVICES, at 1, www.fas.org/sgp/crs/secretary/RS21900.pdf (last accessed May 11, 2013).

[2] 同上註。例如 1966 年「資訊自由法 (Freedom of Information Act, FOIA)」，1995 年「情報授權法 (Intelligence Authorization Act)」，2000 年「公共利益解密法 (Public Interest Declassification Act)」，與 2012 年「減少過度加密法 (Reducing Over-Classification Act)」。

[3] 美國聯邦法規第 32 章 2001 篇，32 C.F.R. 2001, <http://www.law.cornell.edu/cfr/text/32/2001> (last accessed May 11, 2013).

[4] White House, Executive Order 12958 Classified National Security Information (1995), <http://www.fas.org/sgp/clinton/eo12958.html> (last accessed May 11, 2013).

(a) A person may have access to classified information provided that:

(1) a favorable determination of eligibility for access has been made by an agency head or the agency head's designee;

(2) the person has signed an approved nondisclosure agreement; and

(3) the person has a need-to-know the information.

[5] NARA/ISOO, *Classified Information Nondisclosure Agreement (Standard Form 312) Briefing Booklet* (2001), P.1, <http://www.fas.org/sgp/isoo/sf312.html> (last accessed May 11, 2013).

[6] 同上註。

[7] White House, Executive Order 12958 Classified National Security Information (1995), <http://www.fas.org/sgp/clinton/eo12958.html> (last accessed May 11, 2013).

[8] NARA/ISOO, *Implementing Rule of the "Classified Information Nondisclosure Agreement" Subpart B-Prescribed Forms §2003.20(a) (n.d.)*, P.55, http://www.wrc.noaa.gov/wrso/forms/standard-form-312_booklet.pdf (last accessed May 11, 2013).

"SF 312, SF 189, and SF 189-A are nondisclosure agreements between the United States and an individual. The prior execution of at least one of these agreements, as appropriate, by an individual is necessary before the United States Government may grant that individual access to classified information..."

[9] NARA/ISOO, *Classified Information Nondisclosure Agreement (Standard Form 312) Briefing Booklet* (2011), <http://www.fas.org/sgp/isoo/sf312.html> (last accessed May 11, 2013).

[10]同上註。

[11]Western Region Security Office, Protecting Classified Information, http://www.wrc.noaa.gov/wrso/security_guide/intro-4.htm (last accessed May 11, 2013).

[12]Jennifer K. Elsea, The Protection of Classified Information: The Legal Framework (2013) CONGRESSIONAL RESEARCH SERVICES, at 11, www.fas.org/sgp/crs/secrecy/RS21900.pdf (last accessed May 11, 2013).

[13]Jennifer K. Elsea, The Protection of Classified Information: The Legal Framework (2013) CONGRESSIONAL RESEARCH SERVICES, at 11, www.fas.org/sgp/crs/secrecy/RS21900.pdf (last accessed May 11, 2013).

See *Snepp v. United States*, 444 U.S. 507 (1980), noting the remedy in *Snepp* was enforced despite the agency's stipulation that the book did not contain any classified information.

[14]White House, Executive Order 12958 Classified National Security Information (1995), <http://www.fas.org/sgp/clinton/eo12958.html> (last accessed May 11, 2013).

ISOO, National Security Decision Directive No. 84(n.d.), <https://www.fas.org/irp/offdocs/nsdd/nsdd-84.pdf> (last accessed May 11, 2013).

[15]NARA/ISOO, Classified Information Nondisclosure Agreement (Standard Form 312) Briefing Booklet (2001), P.65, http://www.wrc.noaa.gov/wrso/forms/standard-form-312_booklet.pdf (last accessed May 11, 2013).

保密協議曾有SF189與SF189-A版本，與現行SF312版，不論那一版本的保密協議，均經過司法部專家依據當時或現有法律進行審閱，並確認保密協議的合憲性和可執行性。最近有關SF189的訴訟，仍維持保密協議基本的合憲性和合法性。

[16]NARA/ISOO, Classified Information Nondisclosure Agreement (Standard Form 312) Briefing Booklet (2001), P.66-67, http://www.wrc.noaa.gov/wrso/forms/standard-form-312_booklet.pdf (last accessed May 11, 2013).

除憲法上被「視為」符合「可信性 (Trustworthiness)」的下列人員外，其他的人員必須符合三項前提要件（包括簽署保密協議），才得以使用機密資訊。「視為」具「可信性」的人員包括：總統、副總統、國會議員、最高法院法官，與其他由總統提名並經參議院同意的聯邦法院法官，不需以簽署與持已生效的保密契約為條件，即可使用機密資訊。然而，國會議員仍然是以執行職務（立法功能）所「必要 (Need-to-know)」的範圍內為限，例如，該國會議員為負責監督秘密情報部門計畫的委員會，該國會議員與該機關首長，仍必須簽署保密協議或其他類似文件後，才得以使非行政機關人員使用機密資訊。

[17]NARA/ISOO, Classified Information Nondisclosure Agreement (Standard Form 312) Briefing Booklet (2001), P.71, http://www.wrc.noaa.gov/wrso/forms/standard-form-312_booklet.pdf (last accessed May 11, 2013).

[18]NARA/ISOO, Standard Form 312, <http://www.archives.gov/isoo/security-forms/sf312.pdf> (last accessed May 11, 2013).

[19]NARA/ISOO, Implementing Rule of the "Classified Information Nondisclosure Agreement" Subpart B-Prescribed Forms §2003.20(h)(1)&(2) (n.d.), P.56-57, http://www.wrc.noaa.gov/wrso/forms/standard-form-312_booklet.pdf (last accessed May 11, 2013).

[20]White House, Executive Order 12958 Classified National Security Information (1995), <http://www.fas.org/sgp/clinton/eo12958.html> (last accessed May 11, 2013).

Sec. 1.2. Classification Standards.

(a) Information may be originally classified under the terms of this order only if all of the following conditions are met:

- (1) an original classification authority is classifying the information;
- (2) the information is owned by, produced by or for, or is under the control of the United States Government;
- (3) the information falls within one or more of the categories of information listed in section 1.5 of this order; and
- (4) the original classification authority determines that the unauthorized disclosure of the information reasonably could be expected to result in damage to the national security and the original classification authority is able to identify or describe the damage.

Sec. 1.4. Classification Authority.

(e) Exceptional cases. When an employee, contractor, licensee, certificate holder, or grantee of an agency that does not have original classification authority originates information believed by that person to require classification, the information shall be protected in a manner consistent with this order and its implementing directives. The information shall be transmitted promptly as provided under this order or its implementing directives to the agency that has appropriate subject matter interest and classification authority with respect to this information. That agency shall decide within 30 days whether to classify this information. If it is not clear which agency has classification responsibility for this information, it shall be sent to the Director of the Information Security Oversight Office. The Director shall determine the agency having primary subject matter interest and forward the information, with appropriate recommendations, to that agency for a classification determination.

[21]NARA/ISOO, Classified Information Nondisclosure Agreement (Standard Form 312) Briefing Booklet (2001), P.70, http://www.wrc.noaa.gov/wrso/forms/standard-form-312_booklet.pdf (last accessed May 11, 2013).

[22]White House, Executive Order 13526 Classified National Security Information (2009), <http://www.whitehouse.gov/the-press-office/executive-order-classified-national-security-information> (last accessed May 11, 2013).

[23]Jennifer K. Elsea, The Protection of Classified Information: The Legal Framework (2013) CONGRESSIONAL RESEARCH SERVICES, at 5, www.fas.org/sgp/crs/secrecy/RS21900.pdf (last accessed May 11, 2013).

[24]NARA/ISOO, Implementing Rule of the "Classified Information Nondisclosure Agreement" Subpart B-Prescribed Forms §2003.20(h)(3) (n.d.), P.57, http://www.wrc.noaa.gov/wrso/forms/standard-form-312_booklet.pdf (last accessed May 11, 2013).

[25]同上註。

[26]NARA/ISOO, Classified Information Nondisclosure Agreement (Standard Form 312) Briefing Booklet (2001), P.73, http://www.wrc.noaa.gov/wrso/forms/standard-form-312_booklet.pdf (last accessed May 11, 2013).

[27]同上註。

[28]同上註。The terms of the SF 312 specifically state that all obligations imposed on the signer "apply during the time [the signer is] granted

access to classified information, and at all times thereafter.”

[29]同上註。

[30]同上註。

[31]Jennifer K. Elsea, The Protection of Classified Information: The Legal Framework (2013) CONGRESSIONAL RESEARCH SERVICES, at 5, www.fas.org/sgp/crs/secrecy/RS21900.pdf (last accessed May 11, 2013).

[32]同上註， at 11, www.fas.org/sgp/crs/secrecy/RS21900.pdf (last accessed May 11, 2013).

See United States v. Marchetti, 466 F.2d 1309 (4th Cir. 1972).

[33]Jennifer K. Elsea, The Protection of Classified Information: The Legal Framework (2013) CONGRESSIONAL RESEARCH SERVICES, at 11, www.fas.org/sgp/crs/secrecy/RS21900.pdf (last accessed May 11, 2013).

See Haig v. Agee, 453 U.S. 280 (1981).

[34]NARA/ISOO, Classified Information Nondisclosure Agreement (Standard Form 312) Briefing Booklet (2011), <http://www.fas.org/sgp/isoo/sf312.html> (last accessed May 11, 2013).

[35]NARA/ISOO, Classified Information Nondisclosure Agreement (Standard Form 312) Briefing Booklet (2011), <http://www.fas.org/sgp/isoo/sf312.html> (last accessed May 11, 2013) & Jennifer K. Elsea, The Protection of Classified Information: The Legal Framework (2013) CONGRESSIONAL RESEARCH SERVICES, at 10-11, www.fas.org/sgp/crs/secrecy/RS21900.pdf (last accessed May 11, 2013).

失去通過安全檢查的資格可能導致失去政府員工的工作機會；另外，除可能被追討金錢的損害賠償外，該名員工如果亦違反「間諜法（Espionage Act）」與「原子能法（Atomic Energy Act）」的相關條款，還有可能喪失退休金（Retirement Pay）或年金（Annuities）。

[36]NARA/ISOO, Classified Information Nondisclosure Agreement (Standard Form 312) Briefing Booklet (2001), P.74, http://www.wrc.noaa.gov/wrso/forms/standard-form-312_booklet.pdf (last accessed May 11, 2013).

[37]Jennifer K. Elsea, The Protection of Classified Information: The Legal Framework (2013) CONGRESSIONAL RESEARCH SERVICES, at 10, www.fas.org/sgp/crs/secrecy/RS21900.pdf (last accessed May 11, 2013).

[38]Caitlin Tweed, SEAL Team Six Member’s Next Battle Could be in Court (2012), NATIONAL SECURITY LAW BRIEF, <http://nationalecuritylawbrief.com/2012/09/12/seal-team-six-members-next-battle-could-be-in-court/> (last accessed May 11, 2013).

許慧瑩 編譯整理

上稿時間：2014年01月

 推薦文章