Environmental Protection Network

(202) 656-6229
environmentalprotectionnetwork.org
info@environmentalprotectionnetwork.org

EPN Comments on
Confidential Government Information Nondisclosure Agreement
Docket ID OPM-2026-0100
June 26, 2026

The Environmental Protection Network (EPN) harnesses the expertise of more than 750 former Environmental Protection Agency (EPA) career staff and confirmation-level appointees from Democratic and Republican administrations to provide the unique perspective of former regulators and scientists with decades of historical knowledge and subject matter expertise.

EPN respectfully submits this comment in opposition to the Office of Personnel Management's (OPM) proposed government-wide nondisclosure agreement for Federal employees, and urges OPM to withdraw the proposed form, or at a minimum substantially revise and reissue it for a full new public comment period after addressing the serious legal, policy, and practical concerns identified below.

Overview

On May 27, 2026, OPM released for a 30-day public comment period a draft nondisclosure agreement (NDA) potentially impacting all new, current, and past employees. The summary states:

> "The form is intended to document Federal employees' acknowledgment of, and agreement to comply with, current legal obligations to safeguard non-public, confidential, or proprietary information, created or obtained through their official duties, while expressly preserving the right to make disclosures authorized by law. OPM believes that a governmentwide NDA form will promote consistency across Government, better protect confidential information, and better inform Federal employees of their rights and obligations regarding confidential information."

The OPM summary contrasts sharply with our decades of experience[1] handling non-public data. Federal employees who handle classified, confidential unclassified information (CUI), private personal information (PPI), confidential business information (CBI), and other non-public government information are well aware of their obligations and the vast majority rigorously protect the information they possess. Existing laws and training are in place that prevent disclosure. Violators receive adverse personnel and/or legal actions when warranted.

OPM fails to provide evidence that there is a need for the proposed NDA. OPM provides no evidence regarding inconsistencies across Federal agencies in handling non-public information, and ignores the differences inherent to differing types of Federal positions (i.e.; defense, intelligence, civilian and public

[1] If the average EPN volunteer worked 25 years in the Federal government; we have 18,750 person-years of Federal work experience.

trust) and different types of non-public information (i.e.; classified, CUI, PPI, CBI, personnel, grants and contracts, regulatory audits, enforcement).

OPM fails to consider or provide cost estimates of implementing or tracking the use of the NDA across Federal agencies. Even if this NDA offered additional protection for non-public data, it is entirely ineffective at instructing or deterring political appointees who frequently and intentionally leak non-public details for individual or partisan advantage. Instead, the NDA certification—combined with the associated suitability and fitness regulations—could be weaponized to discipline employees based on ambiguous claims of non-disclosure violations. Such claims remain shielded from scrutiny because the broad definition of information subject to non-disclosure includes 'personnel matters.'

OPM ignores congressional limitations on NDAs. Congress has never authorized broad NDAs, limiting NDAs to classified government information and later restricting NDAs to those including specified language. At least one court found unconstitutional nondisclosure forms whose prohibitions were overly broad.

EPN believes that the NDA's sole purpose is to impose a chilling effect upon future, current, and past Federal employees and that it will ultimately reduce the authorized release of government information to the public. OPM should withdraw the proposed NDA from consideration.

We arrive at our conclusions based upon the following considerations:
1. Authorization
2. The proposal is overbroad and ambiguous.
3. The proposal is unnecessary and duplicative.
4. OPM superficially justifies this proposed NDA ignoring past congressional actions and court decisions limiting non-public government information NDAs to classified information.
5. OPM is acting recklessly and maliciously to further harm our Federal workforce that has already been subjected to reassignment, relocation, demotion, termination, buy-outs, and/or administrative leave.
6. The proposal threatens public accountability and would chill protected speech and whistleblowing, further hardening the existing barrier between the Federal government and the public.
7. The proposal does not restrict disclosure of non-public information by political appointees to those who would promote their agenda.
8. It is inappropriate to pre-assign jurisdiction of any claims based on the NDA to a single U.S. District Court.
9. The proposed NDA's "irreparable harm" clause is a coercive, intimidatory tactic.

Detailed information supporting our nine points are provided below.

1. Authorization.

We believe that 5 U.S.C. 3301 and 7301 do not specifically authorize this NDA agreement for all new, current, and past Federal employees. We are unaware of, and OPM has failed to identify, any congressional language authorizing this broad NDA or appropriating funding for it. In contrast, clear and specific authorizations exist pertaining to the nondisclosure of specific types of information such as: Classified Information, CUI, PPI, CBI, personnel records, grants, contracts, investigations, regulatory audits, and enforcement information. For example, within the National Archives and Records Administration (NARA),

specific authorizing language defines CUI and how it is protected and released to the public. No generic NDA is required of Federal workers who handle CUI. Agencies have the option to establish information-specific NDAs if sharing with other agencies or contractors.[2] OPM has failed to identify any congressional authorization that attempts to unify disclosure restrictions across these types of information or the differing types of personnel possessing that information.

Beyond the overly broad claim that the NDA is authorized by 5 U.S.C. 3301 and 7301, OPM cites an Executive Order as sufficient authorization for the NDA.[3] The Executive Order requires the Director of OPM to initiate rulemaking to include additional suitability "criteria including refusal to certify compliance with any applicable nondisclosure obligations, consistent with 5 U.S.C. 2302(b)(13), and failure to adhere to those compliance obligations in the course of Federal employment." Because such a rulemaking would be authorized by Executive Order, not congressional intent, the final rule could be canceled by any future Executive Order or administration. Of interest, rule 2302(b)13 does not require any NDA. Instead, it labels NDAs as a **prohibited personnel practices** if it:

> " … (A) does not contain the following statement: "These provisions are consistent with and do not supersede, conflict with, or otherwise alter the employee obligations, rights, or liabilities created by existing statute or Executive order relating to (1) classified information, (2) communications to Congress, (3) the reporting to an Inspector General or the Office of Special Counsel of a violation of any law, rule, or regulation, or mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety, or (4) any other whistleblower protection. The definitions, requirements, obligations, rights, sanctions, and liabilities created by controlling Executive orders and statutory provisions are incorporated into this agreement and are controlling."; or (B) prohibits or restricts an employee or applicant for employment from disclosing to Congress, the Special Counsel, the Inspector General of an agency, or any other agency component responsible for internal investigation or review any information that relates to any violation of any law, rule, or regulation, or mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety, or any other whistleblower protection."

2. The proposal is overbroad and ambiguous.

The proposed agreement does not adequately define the government information it is trying to protect from disclosure or the government information that is not covered by the NDA and may be disclosed. To the contrary, it covers a sweeping and imprecise category of confidential government information. The notice defines "confidential government information" broadly to include:

> "[A]ll non-public, confidential, or proprietary information, to include, but not be limited to, information relating to internal agency operations, personnel matters, procurement processes, or any

[2] Information Security Oversight Office, NARA PART 2002—CONTROLLED UNCLASSIFIED INFORMATION (CUI), available at https://www.govinfo.gov/content/pkg/CFR-2018-title32-vol6/pdf/CFR-2018-title32-vol6-part2002.pdf

[3] Implementing the President's "Department of Government Efficiency" Workforce Optimization Initiative. EO 14210 February 11, 2025, available at https://www.federalregister.gov/documents/2025/02/14/2025-02762/implementing-the-presidents-department-of-government-efficiency-workforce-optimization-initiative

sensitive, pre-decisional or deliberative material that is not currently publicly available and should not be disclosed under applicable law."

These terms encompass routine workplace communications, policy debates, draft proposals, budget discussions, operational concerns, peer review comments, advisory committee notes, previously unpublished data, and other information that may be important for oversight, public understanding, or lawful whistleblowing.

Perhaps even more concerning, the words "include, but not be limited to" eliminate any kind of boundaries to what non-public, confidential, or proprietary information may be the subject of the NDA, other than a passing nod to certain statutes authorizing disclosure.

The text of the NDA itself is even broader, including "Federal regulation or government-wide policy" as well as "applicable law"; Section 1 of the proposed NDA further adds "rules, regulations and Agency policies and procedures" to the list of what Federal employees must comply with.

The longer the list and the broader the sweep of the requirements and even policies that the NDA incorporates, the more difficult it will be for employees to know exactly whether they are in compliance. With a list this long, the most likely – and probably intended – result would be that employees simply operate under an impermeable cone of silence to avoid the risk of being punished or fired. This is not a good thing for the public or the government.

The overbreadth and vagueness of the NDA will put Federal officials in an impossible situation. It would force Federal employees to guess whether discussing government waste, mismanagement, public health risks, workplace violations, improper political interference, or even an email regarding food in an office pantry could later be characterized as a breach of an NDA. This is especially ironic given OPM's stated purpose to "better inform Federal employees of their rights and obligations regarding confidential information." Indeed, the true purpose appears to be to create a climate of fear in part by being deliberately vague as to what kind of non-public information can be discussed with anyone. This is especially troubling where the covered information may include information that can reveal whether agencies are acting lawfully, honestly, and in the public interest. Furthermore, Federal agencies will, when appropriate, release previously non-public information that are exempt from disclosure under the Freedom of Information Act. An example is a draft rule that could have been protected under the deliberative process privilege, which an agency might choose to release to outside parties for purposes of getting informal input prior to the formal notice and comment process. Any supervisor or high-level political appointee within an agency could categorize deliberative material as policy-related and accuse an employee of violating the NDA certification by disclosing it. Furthermore, given the related suitability and fitness rule that bypasses the Merit Systems Protection Board (MSPB) oversight, it remains unclear what information an employee would even be permitted to access regarding such an accusation.

Although the NDA proposal states that it is intended to document civil service employees' agreement to comply with "current legal obligations" and "not create new substantive restrictions," it appears to go further by attempting to create liability for the disclosure of pre-decisional policymaking statements. For instance, Federal agencies like EPA frequently share 'predecisional or deliberative' materials with partners—including states, localities, industry, and environmental groups—as part of the standard process for developing rules, guidance, and other products. Given this standard practice, prohibiting the disclosure

of such deliberative materials categorically is inappropriate. Such a restriction would exacerbate a culture of fear already surrounding the proposed NDA, coercing employees into silence to avoid potential retribution, and effectively cutting off essential communication channels that are vital for informed public policy development and collaborative governance.

Further, neither the proposal nor the NDA form in the docket makes provision for excluding information critical to disaster assistance and emergency response. How will employees know what information they can release without running afoul of the NDA immediately or in the judgment of supervisors in the future? This may be a critical concern for first responders or the public at large, regarding, for example, toxic or hazardous materials releases or spills, and follow-up monitoring. The need to share information immediately and freely is made clear on National Oceanic and Atmospheric Administration's (NOAA) website discussing information sharing between NOAA and EPA during emergencies:

> "When a disaster occurs, it's critical that the organizations involved in the response can communicate and share information quickly and effectively.
>
> That means groups as diverse and numerous as emergency management, fire service, law enforcement, emergency medical, and responders from local, state, tribal, and Federal governments all need to be on the same page. At NOAA, we're working with our partners to help ensure that the information responders need flows quickly and accurately—when they need it." [4]

Similarly, ARC Facilities, a company in the business of helping organizations to gain instant mobile access to critical incident-related information, also highlights on their website the need for the immediate flow of information:

> "Seconds can be lost in all sorts of ways during an emergency. Time is lost searching for plans, compliance data or other contact information. In the heat of the moment, **a second lost here or there can prove to be the difference between life and death**. **Emergency Info Sharing is more important than ever to protect people, properties and communities**. ARC Facilities has seen firsthand the value of having access to critical information in real time for facilities managers, emergency responders and internal teams to make critical decisions in emergency situations."[5]

Consider a real-world application of these principles from January 2022, when a fertilizer facility storing 600 tons of ammonium nitrate ignited near the Wake Forest University campus.[6] During the subsequent evacuation of approximately 6,500 residents, the Incident Command's decision to manage the incident necessitated real-time data to ensure public safety. The air monitoring data provided by emergency response contractors was vital, directly informing operational decisions, such as when to safely resume campus activities, and providing necessary clarity to the public through media engagement. In such high-stakes environments, the potential for an NDA to induce hesitancy or cause experts to withhold information out of fear of administrative retribution is antithetical to public safety. The prospect that critical data could be

[4] https://blog.response.restoration.noaa.gov/better-chemical-safety-noaa-and-epa-work-improve-data-sharing-during-emergencies

[5] https://www.arcfacilities.com/blog/emergency-info-sharing-strategies-for-fast-crisis-response

[6] Blaze at North Carolina fertilizer plant packed with 600 tons of ammonium nitrate still burning - ABC News

delayed by bureaucratic caution, rather than released as swiftly as it is validated, would create a profound and dangerous chilling effect.

There can certainly be pre-decisional or deliberative material not previously shared outside Federal agencies whose disclosure would be critical during the early hours of an emergency response. Federal emergency response personnel should not be saddled with the burden of deciding if Agency policy and/or Executive Orders do or do not allow them to share - with state, Federal, and local partners or the public - information important to the effective implementation of an emergency response.

The proposed NDA does not distinguish between an *intended* versus *unintended* disclosure of government information. Neither the Federal Register nor the draft NDA distinguish between unintended and intended disclosures of non-public information. Intent is important. Unintended release of government information could result from poorly designed or poorly protected information systems, or even errors by the entity submitting the information to the Federal agency. Such disclosures are not due to negligence or willfulness of the Federal employee in possession of that information. Adverse personnel and legal actions require both intent and adequate proof establishing a legal basis of guilt.

3. The proposal is unnecessary and duplicative.

Federal employees who handle classified information, CUI, private PPI, CBI, and other non-public government information are aware of their obligations to protect the information in their possession. Existing laws and training overwhelmingly prevent intentional non-disclosure.

Federal employees already operate under ethics rules, privacy laws, classification rules, records laws, agency policies and security protocols, disciplinary procedures, security-clearance rules, and whistleblower statutes. OPM has not identified a concrete gap that requires a broad new NDA layered on top of those existing protections.

OPM's notice identifies existing legal obligations as the basis for the proposed form. But if, as OPM claims, Federal employees need a better understanding of the obligations that already exist, the way to address that is effective training, clear guidance, and enforcement of specific laws rather than imposing a broad and ambiguous new agreement that functions as a gag on legitimate disclosure and discourse. The federal government already has established frameworks for classified information, CUI, privacy records, procurement integrity, personnel records, ethics restrictions, and agency-specific security requirements. A generic NDA layered over those frameworks is more likely to confuse employees than to clarify their responsibilities.

4. OPM superficially justifies this proposed NDA, ignoring past congressional actions and court decisions limiting non-public government information NDAs to classified information. A systematic review and assessment of the release of non-public information is required – not a generic NDA.

Beyond Executive Order 14210, OPM's justification for an NDA applicable to all future, current, and past Federal employees relies on scant evidence: only six media-reported examples of non-public information disclosure. Notably, two of these references (7 and 8) are unverifiable. Of the remaining four instances, three involve scenarios where political appointees were as likely to be responsible for the leak as career staff. The

final example, regarding the leak of a Supreme Court draft, could be attributed to any justice, clerk, or staffer with access. Collectively, these isolated and ambiguous incidents fail to provide a credible justification for such a sweeping and intrusive NDA.

The lack of evidence supporting the need for the NDA is remarkable. OPM provides no evidence regarding inconsistencies across Federal agencies in handling information protected by law. Moreover, Federal agencies may properly differ in how they handle non-public information because different agencies are often subject to specific statutes and regulations that impose varying requirements, such as those inherent to differing types of Federal positions (i.e., defense, intelligence, civilian and public trust) and different types of non-public information (i.e., classified, CUI, PPI, CBI, personnel, grants and contracts, regulatory audits, enforcement). For example, Section 14(b)(2) of the Toxic Substances Control Act exempts certain health and safety information from confidential treatment,[7] while the Trade Secrets Act contains no such limitation. Not only is there a lack of evidence supporting the idea that the proposed NDA will increase consistency across Federal agencies or employee understanding to protect non-public data, but such consistency will in some cases conflict with Federal law.

No substantive evidence or assessment is provided documenting how this proposed NDA would decrease inconsistencies across agencies, types of government information, or types of Federal positions (even where such inconsistency is to be avoided). OPM has not provided any evidence demonstrating that this broad new NDA would enhance Federal employees' ability or motivation to protect non-public data beyond the comprehensive legal and ethical frameworks already in place. Implementing this NDA is far more likely to create chaos within agency personnel, security, and ethics offices than to harmonize consistency.

OPM fails to report, intentionally disregards, or is simply unaware of earlier efforts requiring NDAs across all Federal agencies for handling classified information. These failed attempts, limited to classified information, should be seen as a forewarning that expansion across all types of non-public government information will also fail. The Government Accountability Office (GAO) issued a report evaluating Federal agency-wide NDA for classified information in 1991.[8] According to that report:

> "Classified information nondisclosure agreements have long been a source of controversy. Their use has raised complex questions about such issues as the President's ability to protect national security information, the Congress' ability to obtain the information it needs to oversee Federal agencies, and an individual's right to free speech. Use of these agreements has been restricted by the Congress through legislation and challenged by Members of Congress and unions representing government employees in courts of law. In a recent case, a United States District Court generally sustained the government's use of nondisclosure agreements for Federal employees with access to classified information. It … found unconstitutional nondisclosure forms whose prohibitions were overly broad."

Congress took additional action in 2012 when it passed Section 104 of the Whistleblower Protection Enhancement Act.[9] Both the Senate and the House of Representatives made it clear that the purpose of the law was to strengthen protections for whistleblowers because encouraging them to expose waste, fraud, and

[7] 15 U.S.C. 2613(B)(2); 40 CFR Part 703, available at https://www.ecfr.gov/current/title-40/part-703.
[8] Information Security. Federal Agency Use of Nondisclosure Agreement. https://www.gao.gov/assets/nsiad-91-106fs.pdf
[9] Public Law 112-199. https://www.govinfo.gov/content/pkg/PLAW-112publ199/pdf/PLAW-112publ199.pdf

abuse can save money for the government and American taxpayers.[10] MSPB then established the 13th Prohibited Personnel Practice (PPP) specifically limiting NDAs. OPM's inclusion of the language required by Congress and MSPB's establishment of the 13th PPP should not be interpreted as a green light to impose NDAs on all new, current, and past Federal employees. OPM's interpretation that any NDA must include specific language in accordance with the 13th PPP is correct. However, it does not mean that all non-public information should be protected by an NDA or that all Federal workers should have to sign one. OPM's belief that Congress has no ongoing interest in NDAs or has capitulated its role related to NDAs to the Executive Branch may be in for a rude awakening. Clearly, OPM must be aware that Congress has neither authorized legislation, nor appropriated the needed funds, to develop and implement the proposed NDA.

OPM ignores the costs associated with NDAs just for classified information. According to the 1991 GAO report, costs to implement the signing of NDAs across Federal agencies during one year was approximately $4,279,000 in 2026 dollars.[11] In 1987, Congress restricted appropriations for NDAs …

> "In December 1987, the Congress included language prohibiting the continued use of Standard Form 189 and Form 4193 in the "Treasury, Postal Service, and General Government Appropriations Act, 1988." Section 630 of the act states that No funds appropriated in this or any other act for fiscal year 1988 may be used to implement or enforce the agreements in Standard Form 189 and Form 4193 of the Government or any other nondisclosure policy, form, or agreement if such policy, form, or agreement: (1) concerns information other than that specifically marked as classified; or, unmarked but known by the employee to be classified; or, unclassified but known by the employee to be in the process of classification determination…"

Over the years, GAO and Office of the Inspector General (OIG) offices have investigated a number of alleged disclosures of confidential information. OPM has failed to cite those reports, presumably because they do not support OPM's proposal. EPN has reviewed four such reports, and while they deal with cases in which information may have been improperly released, none recommended either an NDA directed at the

[10] Prohibited Personnel Practice 13: Nondisclosure Forms, Policies, & Agreements. https://www.mspb.gov/ppp/13ppp.htm
[11] Information Security. Federal Agency Use of Nondisclosure Agreement. https://www.gao.gov/assets/nsiad-91-106fs.pdf

specific government agency, information type, or personnel involved in a documented disclosure.[12] No generic NDA like that proposed by OPM has been recommended by an OIG or the GAO.

Given the breadth, cost, potential risk, and both judicial and congressional experience with NDAs, a systematic and independent evaluation is required to establish improvements in securing non-public information. The rush to implement this NDA is simply putting the cart before the horse, where the cart is the NDA and the horse is an unidentified problem lacking an evidence-based solution. An evaluation should review all available literature including GAO and OIG reports and decisions. The review should determine risk levels for disclosure across Federal information types and personnel types (including political appointees), evaluate the effectiveness of current rules and regulations designed to prevent disclosures, and determine the cost and effectiveness of the proposed solution to reduce the scope of the problem.

5. OPM is acting recklessly and maliciously to further harm our Federal workforce that has already been subjected to reassignment, relocation, demotion, termination, buy-outs, and/or administrative leave.

EPN believes that the NDA's sole purpose is to impose a chilling effect upon future, current, and past Federal employees and will ultimately reduce the authorized release of government information to the public. The proposed agreement risks creating confusion, chilling lawful disclosures, discouraging employees from reporting misconduct, and weakening public accountability.

It is reckless to publish this proposed NDA without having thoroughly reviewed and described authoritative reports, past congressional and judicial actions on global classified NDAs, acknowledging the costs associated with the NDA, or evaluating its usefulness and effectiveness. The fact that this inadequate proposal is limited to a 30-day public comment review despite past congressional actions, the MSPB's establishment of the 13th PPP, the associated costs, and the lack of an authorization or appropriation highlights the fact that OPM only cares about fulfilling Executive Order 14210, without regard to the legal, financial, practical, and harmful flaws in the proposal. OPM has turned a blind eye towards the harm that

---

[12] An audit of 1,694 IRS investigations into the willful unauthorized access of tax data by employees—and 27% were found to be violations. Most of these violations resulted in the offending employee's suspension, resignation, or removal. (IRS Security of taxpayer information: Characteristics of employee unauthorized access and disclosure cases. May 2022. https://www.gao.gov/products/gao-22-105872).
An audit of the Department of Health and Human Services COVID-19 IT systems included 99 systems that collect, store, and protect personally identifiable information (PII). (COVID-19: HHS Needs To Identify Duplicative Pandemic IT Systems and Implement Key Privacy Requirements.GAO-24-106638, September 2024, https://www.gao.gov/products/gao-24-106638).
The Federal Trade Commission (FTC) OIG released a report assessing 23 potential leaks involving non-public FTC information that appeared in media publications. Identified patterns coincided with leadership changes and policy debates. No responsible individual was identified (FTC OIG Investigation Summary 5.11.26, https://oig.ftc.gov/reports/ftc-oig-investigates-disclosure-ftc-nonpublic-information-media).
The US Department of Education OIG reported on an investigation of three incidents in which there appeared to be unauthorized releases of non-public information to the *Washington Post* and/or *Politico*.# This report highlights deficiencies within DOE for protecting the release of non-public data and emphasizes the difference between types of non-public data (Unauthorized Release of Non-Public Information Control No ED-OIG/X42S0001 (P17Mar30122), March 2018, https://oig.ed.gov/sites/default/files/reports/2025-06/FY18X42S0001031224v100SECURED.pdf).

the NDA would do to Agencies that will implement the proposal and the Federal workforce OPM is charged with protecting and supporting.

The list of ten questions that OPM considers appropriate for comment reinforces the farcical nature of this short comment period. OPM does not seek evidence for the need or justification of the NDA. OPM does not seek broad input into the benefits or costs of establishing the NDA. The information OPM seeks is limited to fine tuning an overly broad, potentially dangerous weapon that it plans to hang over the head of Federal workers as a threat. The questions clearly show that OPM intends to move forward regardless of the potential harm, cost, or public concern.

6. The proposal threatens public accountability and would chill protected speech and whistleblowing, further hardening the existing barrier between the Federal government and the public.

The public has a strong interest in transparent, accountable government. Federal employees are often the first to recognize waste, abuse, unlawful conduct, threats to public safety, or pressure to distort science, law, policy, or data. A broad NDA could deter employees from seeking help, communicating with oversight bodies, cooperating with Congress, or making protected disclosures through lawful channels. The result would be less accountability, not more responsible government.

Systems must be established that guarantee confidentiality or anonymity to ensure that government employees can safely report information regarding waste, abuse, unlawful conduct, threats to public safety, or pressure to distort science, law, policy, or data. A recent GAO report examining disclosures from outside the government to regulatory agencies highlights the dangers of overbroad NDAs in industry and the need to protect workers who disclose the information.[13] Any attempt to limit disclosure conflicts with a variety of legal authorities that protect the right of Federal employees to share important information. These range from the First Amendment to specific statutes including the Whistleblower Protection Act, the Inspector General Act, the merit system principles at 5 U.S.C. 2301(b)(9), EPA's "fishbowl" policy, and the Sixth Amendment right to counsel.[14]

The proposal states that it preserves disclosures authorized by law, by citing the Whistleblower Protection Act and restating verbatim the terms of 5 U.S.C. s. 2302(b)(13). This may technically satisfy the regulations on prohibited personnel practices, but is hardly sufficient to prevent a chilling effect. Employees who are told to sign a broad, permanent, legally significant NDA may reasonably fear discipline, removal, civil liability, or referral for investigation if they disclose information that agency leadership later considers embarrassing or inconvenient. Moreover, the body of law relating to what information disclosures are protected is complex; simply citing or generally alluding to those laws does not provide employees the guidance they would need to be certain they were in compliance with the NDA. By requiring all Federal employees to sign an NDA that categorically prohibits such disclosure (even if such a blanket disclosure ban were lawful), the NDA would prevent not only individual employees but even agencies from performing normal functions that advance the agency's mission.

---

[13] Protections For Whistleblowers and Others: Selected Agency Actions Regarding Reports of Wrongdoing. GAO March 2026, GAO-26-107650, available at https://files.gao.gov/reports/GAO-26-107650/index.html

[14] EPN here draws from and concurs with the comments on this OPM proposal of Public Employees for Environmental Responsibility (PEER), available at https://peer.org/wp-content/uploads/2026/06/2026_06_16-PEER-Comments-NDA-OPM-2026_0100-0004.pdf .

Whistleblower protections are effective only when employees understand and trust that they can use them without retaliation. A governmentwide NDA that emphasizes secrecy while relying on general legal carveouts risks sending the opposite message: that employees should remain silent unless they are certain, at their own peril, that a disclosure is protected. That result would undermine Congress' judgment that Federal employees must be able to report violations of law, gross mismanagement, gross waste of funds, abuse of authority, and substantial dangers to public health or safety.

The proposal requests comment on the appropriate consequences to take if existing employees choose not to sign the NDA. The NDA form in the docket notes that "failure to sign may result in removal from Federal service and potential debarment," making clear that this is being instituted as a legal requirement, not merely an information collection exercise exempt from the Paperwork Reduction Act. And civil and criminal penalties are cited as potential remedies for violation of an NDA. All of these statements are likely to chill legitimate disclosures, protected speech, as well as Whistleblower activities.

OPM's notice includes a proposed NDA that claims to be voluntary but in Orwellian fashion undermines that claim by warning that failure to sign may result in removal from Federal service and potential debarment (barring an individual from Federal employment or contractor status for a period of time). It is critical to evaluate the proposed NDA in the context of two other questionable OPM rulemakings related to Federal suitability and fitness assessments. First, OPM has introduced a Suitability and Fitness regulation[15] —currently nearing finalization—which expands suitability criteria to encompass post-employment behavior and reclassifies failure to adhere to nondisclosure requirements as a suitability concern. OPM projections indicate that this could shift approximately 50 percent of removals currently managed via Civil Service Reform Act adverse-action procedures into the suitability framework. Second, OPM has proposed a Suitability Action Appeals rule[16] that would strip appeals of their current oversight by MSPB, transferring them to OPM. In combination, the proposed NDA and these rulemakings create a structure where accusations of leaks, non-compliance, or a refusal to sign could trigger removal and debarment through a process that severely lacks the robust, independent protections Federal employees rely on.[17]

7. The proposal does not restrict disclosure of non-public information by political appointees.

By failing to specifically include political appointees, who are frequently responsible for the unauthorized disclosure of highly sensitive and classified information, the proposed NDA creates an arbitrary distinction. This omission directly contradicts the stated rationale of the proposal and suggests that its true intent may be something other than the protection of government information.

Relevant examples include:

[15] Published June 3, 2025 (90 FR 23467), available at https://www.govinfo.gov/content/pkg/FR-2025-06-03/pdf/20
[16] Published February 6, 2026 (91 FR 5352), available at https://www.govinfo.gov/content/pkg/FR-2026-02-06/pdf/2026-02449.pdf
[17]EPN here draws from Civil Service Strong's comment guide , available at https://cdn.prod.website-files.com/6752b77479a4a21a9253956b/6a26e7cb37b4cb61b6cecdaa_S7eDoOo0gUIBNHq8Rs_itEkaInnYbXIfL0b3kcjU0KQ.pdf

- On March 11-15, 2025, when U.S. national security leaders were observed on a group chat using the Signal messaging service, conversing about imminent military operations against the Houthis in Yemen, code-named Operation Rough Rider.[18]
- In Summer 2025, Madhu Gottumukkala uploaded sensitive contracting documents into a public version of ChatGPT triggering automatic security warnings to stop the theft or unintentional disclosure of government information.[19]
- In 2023, reports emerged of a 2021 audio recording capturing Donald Trump discussing a classified Pentagon document regarding a potential U.S. attack on Iran. During the conversation at his Bedminster, New Jersey, golf club, Trump referenced a "highly confidential" plan and acknowledged he could no longer declassify it because he was out of office.
- The CIA leak scandal when political appointees of the Bush Administration leaked classified information to the Washington Post that Valerie Plame was a CIA agent.[20]
- Miles Taylor, a former Department of Homeland Security (DHS) chief of staff in Trump's first term leaked information. He authored a 2018 anonymous op-ed and later the 2019 book *A Warning*, both titled "Anonymous," which described an internal resistance working to thwart Trump's agenda.

8. It is inappropriate to pre-assign jurisdiction and venue of any claims based on the NDA to a single U.S. District Court.

The proposed NDA states, "[b]oth Employee and Agency understand that the U.S. District Court for the District of Columbia is an appropriate forum for any claims based on or arising from this Agreement, including the breach thereof, and consent to venue and personal jurisdiction in that court." In many cases, Federal statutes provide where jurisdiction and venue lie for specific types of challenges, and the NDA cannot override that. Even where no such statutory constraints exist, OPM does not even attempt to justify the implausible argument that requiring a Federal employee to restrict their available jurisdiction and venue choices in a future legal action somehow better protects information subject to protection under law.

9. The proposed NDA's "irreparable harm" clause is a coercive, intimidatory tactic.

The NDA would require Federal employees to concede in advance the magnitude and effect of unspecified future disclosures, to the possible detriment of the employees: "The Employee understands that a breach or threatened breach of this Agreement would cause irreparable harm to the Agency for which monetary damages would be an inadequate remedy." Such language is again intended to intimidate rather than protect information. Moreover, a "threatened breach" is not a breach, and has nothing to do with an employee's duty to actually protect information.

Conclusion

In summary, EPN strongly opposes the OPM's proposed government-wide NDA. This proposal is fundamentally flawed, lacks the necessary congressional authorization, and fails to provide a substantiated evidence base to justify its implementation. Rather than enhancing the protection of non-public government

[18] https://en.wikipedia.org/wiki/United_States_government_group_chat_leaks
[19] https://www.politico.com/news/2026/01/27/cisa-madhu-gottumukkala-chatgpt-00749361
[20] https://en.wikipedia.org/wiki/Plame_affair

information, this NDA introduces overbroad and ambiguous requirements that will inevitably result in a chilling effect on the Federal workforce.

By creating a climate of fear, the proposed agreement threatens to undermine essential whistleblower protections, discourage legitimate internal and public oversight, and impede the critical flow of information during emergency response and policy development. The NDA prioritizes intimidation over clarification, creates potentially coercive legal hurdles for employees, and fails to address the very issue it claims to solve: the unauthorized disclosure of sensitive information by political appointees.

EPN urges OPM to withdraw this proposal immediately. If OPM's true intent is to improve compliance with existing obligations, the path forward is through robust training, clear communication, and the enforcement of established laws—not through the imposition of a punitive, duplicative, and legally questionable agreement that weakens public accountability and trust in our Federal institutions.