

## SF-328 60 Day FRN Public Comments Requiring Response

(note: all typos are how they appeared on the Register)

1. As an FSO with 30 years of NISP experience with large 100K+ companies through tiny FCLs, I would like to provide the following comments to the proposed revised and expanded SF328:

Subject: CUI Protection

Impact: Administrative

Comment: Per the DoD and NARA CUI Marking guide, the designation indicator/distribution statements should be placed on the first page, vice page two.

Recommended Mitigation: If CUI protection is required, place the designation indicator at the bottom of the first page

**RESPONSE:** Due to spacing issues the CUI designator indicator is placed on the second page. The Marking Guide indicates the designation indicator must be readily apparent and may appear only on the first page or cover. It does not mandate it must appear on the first page, but provides an option to only appear on the first page instead of each subsequent page.

2. As an FSO with 30 years of NISP experience with large 100K+ companies through tiny FCLs, I would like to provide the following comments to the proposed revised and expanded SF328:

Subject: Aggregated Foreign Ownership

Impact: Substantive

Comment: Per guidance "If 5 percent or greater interest is held, in aggregate, by multiple foreign person(s) from the same foreign country or within affiliated entities, identify each foreign interest and overall percentage of ownership from such entities..." While identifying this information should be possible for private entities, publicly traded corporations, might find this requirement challenging, especially for excluded parents, as they do not currently collect the information required to determine aggregated ownership. They are provided with SEC 13D/G for any 5% owners and some companies will conduct limited research on the top 10, 40, 100 owners. However, the required due diligence to state there are no aggregated ownership may be challenging

Recommended Mitigation: Consider providing guidance for due diligence required to respond to this question.

**RESPONSE:** Each respondent is required to use reasonably good faith efforts to respond fully and accurately to each question. The instructions have been modified to reflect this standard.

3. As an FSO with 30 years of NISP experience with large 100K+ companies through tiny FCLs, I would like to provide the following comments to the proposed revised and expanded SF328:

Subject: Material Change

Impact: Substantive

Comment: There is no substantive 32 CFR 117, DCSA, ISL or government wide published definition of "material change." 32 CFR 117.8(c)(7)(v) states "When submitting this information, it is not necessary to repeat answers that have not changed." However, it is unclear if that refers to the overall Yes/No or the specific remarks which will (for most companies) change consistently. Without clear guidance, some companies will unintentionally under report, while others will over report for minor details that do not change FOCI concerns.

Recommended Mitigation: Consider providing guidance for the "material changes" as that will be a critical reporting requirement.

**RESPONSE:** This comment is not specific to the form. Changes requiring filing are included in 32 CFR Part 117. No change will be made to the form at this time.

4. As an FSO with 30 years of NISP experience with large 100K+ companies through tiny FCLs, I would like to provide the following comments to the proposed revised and expanded SF328:

Subject: Excluded Parent Marking

## SF-328 60 Day FRN Public Comments Requiring Response

Impact: Administrative

Comment: The form does not provide any visible means to indicate if SF328 is for an excluded parent, nor which entity the form is to be associated with.

Recommended Mitigation: Consider adding a field on page two to indicate is this is a covered entity or excluded parent and which cage codes are associated with this form.

**RESPONSE:** The form is filed within established systems that attach them to specific files. The use of excluded parent SF-328s is not consistent across Cognizant Security Agencies or Office or programs in which this form may be used. Therefore, no change will be made at this time for this comment.

5. As an FSO with 30 years of NISP experience with large 100K+ companies through tiny FCLs, I would like to provide the following comments to the proposed revised and expanded SF328:

Subject: Excluded Parent Guidance

Impact: Substantive

Comment: DCSA typically and informally allows for broader responses for excluded parents as the potential FOCl is reduced by the established exclusion. That tolerance is not provided in guidance or documentation.

Recommended Mitigation: Consider providing guidance for the expected details for excluded parents

**RESPONSE:** The submission requirements are the same for each entity that is required to complete the SF-328 whether they are an excluded parent or not. The use of excluded parent SF-328s is not consistent across Cognizant Security Agencies or Office or programs in which this form may be used. Therefore, no change will be made at this time for this comment.

6. As an FSO with 30 years of NISP experience with large 100K+ companies through tiny FCLs, I would like to provide the following comments to the proposed revised and expanded SF328:

Subject: Net Income

Impact: Substantive

Comment: Per Question 7 "total revenue or net income from any single foreign person" We are unable to imagine a reasonable scenario where % of net income could be associated with a specific foreign person.

Recommended Mitigation: Consider removing "net income" from the question and guidance

**RESPONSE:** There are instances where net income is associated with a specific foreign person. In addition, the general accounting practices of industry result in varying degrees of response to this question depending on their focus on revenue or income. Therefore, this question is written to capture all permutations that might create a FOCl risk. Net income will not be removed from the form or instructions at this time.

7. Substantive: While the SF328 is due for review, the new form itself has not been released. Until the Form and the associated instructions are released we are unable to provide substantive comments for review.

**RESPONSE:** On May 19, 2024, DCSA provided the revised SF-328 to industry groups and associations for dissemination to its members, as applicable, including the National Industrial Security Program Policy Advisor (NISPPAC) for industry, The Society of Industrial Security Professionals (NCMS), National Defense Industrial Association (NDIA), and Aerospace Industries Association (AIA). In addition, if any individuals reached out to DCSA to obtain the revised SF-328, DCSA provided those personnel a copy of the proposed new SF-328.

8. As an FSO with 30 years of NISP experience with large 100K+ companies through tiny FCLs, I would like to provide the following comments to the proposed revised and expanded SF328:

## SF-328 60 Day FRN Public Comments Requiring Response

Subject CUI Markings

Impact: Administrative

Comment: Per the DoD and NARA CUI Marking guide, the designation indicator/distribution statements should be placed on the first page, vice page two.

Recommended Mitigation: If CUI protection is required, place the designation indicator at the bottom of the first page

**RESPONSE:** Due to spacing issues the CUI designator indicator is placed on the second page. The Marking Guide indicates the designation indicator must be readily apparent and may appear only on the first page or cover. It does not state it must be included on the first page.

9. As an FSO with 30 years of NISP experience with large 100K+ companies through tiny FCLs, I would like to provide the following comments to the proposed revised and expanded SF328:

Subject: Foreign-derived Products or Services

Impact: Critical

Comment: Per guidance “There is no expectation for the contractor to ask every customer, vendor, person, or other similar organizations...” However, some of the following requirements “must be fully identified in all circumstances: All suppliers of foreign-derived products or services used in the performance of classified or U.S. government contracts or agreements.” The identification of foreign-derived products or services is vastly broader than any other government supply chain reporting requirements and will be a substantial increase in reporting requirements for almost every company. For example, a company providing support to the US Government in a foreign country would under this definition be required to “fully identify” every service provider (from lodging to water). Gathering and maintaining the information requested would lead to a substantial increase in contract requirements.

Recommended Mitigation: Consider revising guidance from “fully identified in all circumstances” to “substantially aids your organization's operations” or providing further clarifications to limit no substantive/non-material support.

**RESPONSE:** Each respondent is required to use reasonably good faith efforts to respond fully and accurately to each question. The instructions have been modified to reflect this standard. The defense industrial base is expected to maintain a reasonable level of awareness pertaining to its use of foreign vendors supporting U.S. government contract performance. The required information is limited to foreign products or services used in the performance of classified or USG efforts.

10. As an FSO with 30 years of NISP experience with large 100K+ companies through tiny FCLs, I would like to provide the following comments to the proposed revised and expanded SF328:

Subject: Foreign Persons substantially aids

Impact: Critical

Comment: Per guidance “Foreign persons providing information technology, recruiting, human resources, accounting, finance, legal, manufacturing, business development, technological know-how, or any other service which substantially aids your organization's operations” It is unclear if “substantially aids applies only to any other service or to the entire list.

Recommended Mitigation: Consider moving substantially aids...to immediately after Foreign persons in the beginning of the paragraph to remove any confusion.

**RESPONSE:** The instructions require the identification of all foreign persons providing the services listed. In addition to the services listed, the contractor is further required to identify foreign persons providing any additional services, outside of those mentioned, which substantially aid the organization's operations. Wording has been changed to make this distinction clearer.

11. As an FSO with 30 years of NISP experience with large 100K+ companies through tiny FCLs, I would like to provide the following comments to the proposed revised and expanded SF328:

## SF-328 60 Day FRN Public Comments Requiring Response

Subject: Academic Institution Foreign research agreements/exchanges

Impact: Critical

Comment: Per guidance "Research agreements...Faculty/student academic, cultural, talent or other exchange programs with foreign person" must be identified. For the vast majority of academic institutions this would require updates to the SF328 constantly. While the first two questions allow for broad %/country responses the second two questions require details by name reporting which would constantly be changing.

Recommended Mitigation: Consider revising guidance or providing further clarifications to limit no substantive/non-material support.

**RESPONSE:** SF-328 material change reporting requirements are outlined in 32 CFR 117.8(c)(7)(v). In addition, each Cognizant Security Agency or Office or other program using this form are best positioned to provide additional guidance, as appropriate. No changes to this form or instructions will be made at this time. DCSA will examine the impacts this new form has on submissions and issue guidance through appropriate channels, if necessary.

12. As an FSO with 30 years of NISP experience with large 100K+ companies through tiny FCLs, I would like to provide the following comments to the proposed revised and expanded SF328:

Subject: Foreign-derived Products or Services

Impact: Critical

Comment: Per guidance "There is no expectation for the contractor to ask every customer, vendor, person, or other similar organizations..." However, some of the following requirements "must be fully identified in all circumstances: All suppliers of foreign-derived products or services used in the performance of classified or U.S. government contracts or agreements." The identification of foreign-derived products or services is vastly broader than any other government supply chain reporting requirements and will be a substantial increase in reporting requirements for almost every company. For example, a company providing support to the US Government in a foreign country would under this definition be required to "fully identify" every service provider (from lodging to water). Gathering and maintaining the information requested would lead to a substantial increase in contract requirements.

Recommended Mitigation: Consider revising guidance from "fully identified in all circumstances" to "substantially aids your organization's operations" or providing further clarifications to limit no substantive/non-material support.

**RESPONSE:** Each respondent is required to use reasonably good faith efforts to respond fully and accurately to each question. The instructions have been modified to reflect this standard. The defense industrial base is expected to maintain a reasonable level of awareness pertaining to its use of foreign vendors supporting U.S. government contract performance. The required information is limited to foreign products or services used in the performance of classified or USG efforts.

13. As an FSO with 30 years of NISP experience with large 100K+ companies through tiny FCLs, I would like to provide the following comments to the proposed revised and expanded SF328:

Subject: Foreign Persons

Impact: Substantive

Comment: Per the second note "unless otherwise stated, the definitions of terms in this form are the same as those found in 32 CFR 117.3." However, the term foreign person(s) is THE critical term for this entire form and requires the submitter to travel from 117 to 800.224 to 800.208 and is a constant discussion amongst even experienced NISP counsels. Most companies focus on the foreign ownership and neglect to review foreign control. Without clear guidance, some companies will unintentionally under report, while others will over report for minor details that do not change FOCI concerns. Although Foreign Persons is defined at the end of the guidance, as the definition might be missed at the end.

Recommended Mitigation: Consider providing initial guidance for the "foreign persons" to clarify

## SF-328 60 Day FRN Public Comments Requiring Response

foreign control as defined by 800.224 and 800.208 are as important as foreign ownership. This will reduce additional information/clarification requests from DCSA FO CI analysts.

**RESPONSE:** This comment is not germane to this form or the instructions.

14. As an FSO with 30 years of NISP experience with large 100K+ companies through tiny FCLs, I would like to provide the following comments to the proposed revised and expanded SF328:

Subject: Foreign Persons substantially aids

Impact: Critical

Comment: Per guidance "Foreign persons providing information technology, recruiting, human resources, accounting, finance, legal, manufacturing, business development, technological know-how, or any other service which substantially aids your organization's operations" It is unclear if "substantially aids applies only to any other service or to the entire list.

Recommended Mitigation: Consider moving substantially aids...to immediately after Foreign persons in the beginning of the paragraph to remove any confusion.

**RESPONSE:** The instructions require the identification of all foreign persons providing the services listed. In addition to the services listed, the contractor is further required to identify foreign persons providing any additional services, outside of those mentioned, which substantially aid the organization's operations. Wording has been changed to make this distinction clearer.

15. As an FSO with 30 years of NISP experience with large 100K+ companies through tiny FCLs, I would like to provide the following comments to the proposed revised and expanded SF328:

Subject: Foreign Persons

Impact: Substantive

Comment: Per guidance "Foreign persons providing information technology, recruiting, human resources, accounting, finance, legal, manufacturing, business development, technological know-how, or any other service which substantially aids your organization's operations" Some companies may have difficulty identifying employee that are foreign persons vice the currently collected US/non-US persons.

Recommended Mitigation: Consider the impact of foreign persons/vice non-US persons reporting requirements.

**RESPONSE:** Services can be provided by non-U.S. persons, but it can also be provided by foreign companies, countries, etc., in addition to foreign nationals. The term foreign person appropriately encapsulates all potential sources for the identified services.

16. Question: If the C3PAO are not currently undergoing the FO CI risk review, what happens to companies that get certified by a C3PAO that subsequently fails the enhance FO CI review (e.g. a company gets certified then the C3PAO gets bought and fails FO CI)?

**RESPONSE:** This comment is not germane to this form or the instructions. That question should be directed to the DoD CMMC Program Office to address.

Question: Will existing C3PAO's have an obligation to disclose possible acquisition by a foreign entity ahead of sharing past assessment data?

**RESPONSE:** This comment is not germane to this form or the instructions. That question should be directed to the DoD CMMC Program Office to address.

Question: Will changes to the 328 be incorporated into Section 847 of the National Defense Authorization Act?

## SF-328 60 Day FRN Public Comments Requiring Response

RESPONSE: It is unclear as to the point of this question. However, we believe the question is asking whether this new SF-328 will be used for purposes of conducting FY20 NDAA Section 847, or DoDI 5205.87 reviews. If that is the case, yes, as indicated in provision #2 of the form, it will be used to collect FOCI information for the purpose of Section 847.

17. As an FSO with 30 years of NISP experience with large 100K+ companies through tiny FCLs, I would like to provide the following comments to the proposed revised and expanded SF328:

Subject: Supporting Documents

Impact: Administrative

Comment: Per the Note: "All responses referencing supporting documentation must include the name and date of the document, and specific page number, section, or paragraph supporting each response." However, it is unclear if changes to the supporting documentation require new signatures and dates to the SF-328 itself. DCSA has allowed substantive changes to the SF328 documentation without the SF328 resigned. This presents the potential for substantive changes to the submission without concurrence by the authorized representative.

Recommended Mitigation: DCSA needs to consider if they should accept changes to the supporting documentation without the concurrence of the authorized representative and provide clarifying guidance.

RESPONSE: This comment is not germane to this form or the instructions. However, the supporting documentation for specific SF-328 questions does not typically include documentation which is subject to change regularly, such as corporate governance documentation. Substantive changes to the supporting documentation for the SF-328 would likely result in a material change IAW 32 CFR Part 117. The Facility Security Officer is an authorized representative of the company regarding security matters and submission of material changed condition packages for DCSA.

18. As an FSO with 30 years of NISP experience with large 100K+ companies through tiny FCLs, I would like to provide the following comments to the proposed revised and expanded SF328:

Subject CUI Protection

Impact: Critical

Comment: "CUI when filled in" is a challenging marking as it is directive, and once information is provided, the document requires CUI protection. While most FSOs have access to a CUI endpoint, many SMOs/Finance/Corp Support do not. Additionally, for excluded parents, new to DoD entities, and non-DoD FCLs they will not otherwise have a CUI/CMMC DFARS requirement to protect CUI. CUI-Proprietary information is challenging as, per both DoD and NARA CUI includes non-classified information that an entity creates or possesses for or on behalf of the government. Additionally, most definitions state CUI is CUI upon creation, vice upon submission to the government. Without clarification/additional guidance, this CUI protection requirement will be uniquely extensive and costly for companies across the DiB.

Recommended Mitigation: Reconsider CUI when filled in markings. Coordinate with DCSA CUI Policy office to determine appropriate protections and markings.

RESPONSE: Due to the nature of the content submitted with this form, it becomes CUI once the company populates it with their proprietary information and submits it to a government party. It is not CUI when in the possession of the company whose proprietary information it is. Unfortunately, there is no practical way that the government can ensure the appropriate markings are applied to this form in transit or once received that ensures its marking and protection. Furthermore, there is no additional banner marking that can be used to distinguish at which point this form must be handled as CUI for which parties. However, an adjustment has been made to provision #6 to add clarifying language concerning when it becomes CUI.

19. As an FSO with 30 years of NISP experience with large 100K+ companies through tiny FCLs, I would like to provide the following comments to the proposed revised and expanded SF328:

## SF-328 60 Day FRN Public Comments Requiring Response

Subject: Supporting Documents

Impact: Administrative

Comment: Per the Note: "All responses referencing supporting documentation must include the name and date of the document, and specific page number, section, or paragraph supporting each response." However, it is unclear if changes to the supporting documentation require new signatures and dates to the SF-328 itself. DCSA has allowed substantive changes to the SF328 documentation without the SF328 resigned. This presents the potential for substantive changes to the submission without concurrence by the authorized representative.

Recommended Mitigation: DCSA needs to consider if they should accept changes to the supporting documentation without the concurrence of the authorized representative and provide clarifying guidance.

RESPONSE: This comment is not germane to this form or the instructions. However, the supporting documentation for specific SF-328 questions does not typically include documentation which is subject to change regularly, such as corporate governance documentation. Substantive changes to the supporting documentation for the SF-328 would likely result in a material change IAW 32 CFR Part 117. The Facility Security Officer is an authorized representative of the company regarding security matters and submission of material changed condition packages for DCSA.

20. As an FSO with 30 years of NISP experience with large 100K+ companies through tiny FCLs, I would like to provide the following comments to the proposed revised and expanded SF328:

Subject CUI Protection

Impact: Critical

Comment: "CUI when filled in" is a challenging marking as it is directive, and once information is provided, the document requires CUI protection. While most FSOs have access to a CUI endpoint, many SMOs/Finance/Corp Support do not. Additionally, for excluded parents, new to DoD entities, and non-DoD FCLs they will not otherwise have a CUI/CMMC DFARS requirement to protect CUI. CUI-Proprietary information is challenging as, per both DoD and NARA CUI includes non-classified information that an entity creates or possesses for or on behalf of the government. Additionally, most definition state CUI is CUI upon creation, vice upon submission to the government. Without clarification/additional guidance, this CUI protection requirement will be uniquely extensive and costly for companies across the DiB.

Recommended Mitigation: Reconsider CUI when filled in markings. Coordinate with DCSA CUI Policy office to determine appropriate protections and markings.

RESPONSE: Due to the nature of the content submitted with this form, it becomes CUI once the company populates it with their proprietary information and submits it to a government party. It is not CUI when in the possession of the company whose proprietary information it is. Unfortunately, there is no practical way that the government can ensure the appropriate markings are applied to this form in transit or once received that ensures its marking and protection. Furthermore, there is no additional banner marking that can be used to distinguish at which point this form must be handled as CUI for which parties. However, an adjustment has been made to provision #6 to add clarifying language concerning when it becomes CUI.