

# How to Conduct Regulatory Due Diligence with Domain Intelligence: DIY Domain Research Suite (DRS) Guide

Posted on January 3, 2023

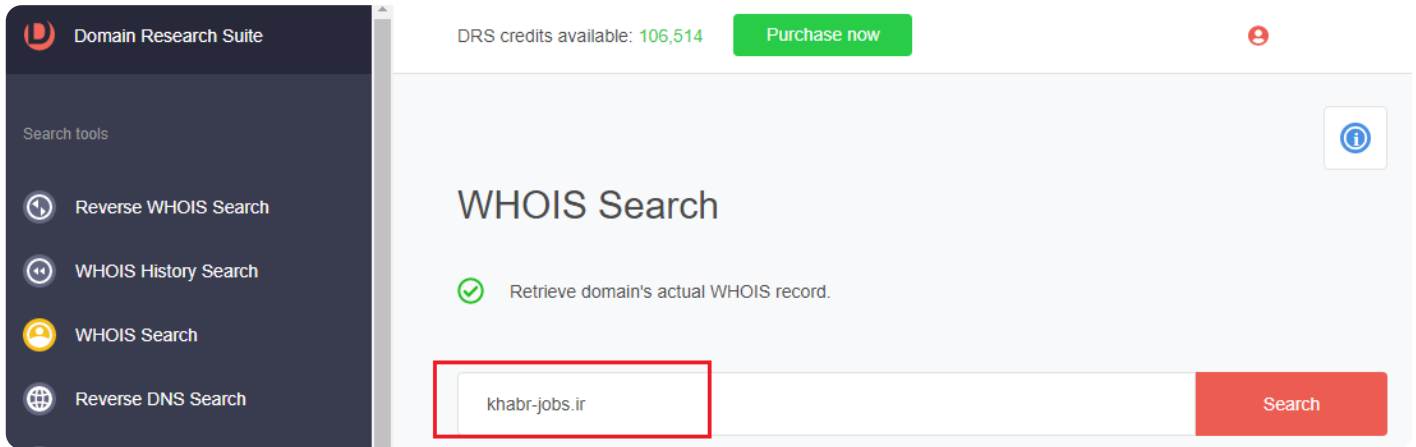
Businesses worldwide must follow certain regulations typically defined by different government agencies and international organizations. Otherwise, they may face legal issues and notably be levied with monetary fines.

DNS intelligence can help businesses conduct regulatory due diligence through domain research and monitoring techniques. How? We'll take you through the process using the [Domain Research Suite \(DRS\)](#) and information provided by the Office of Foreign Assets Control (OFAC), so you can also perform the same screening for your company.

## Step #1: Screen Domains Using Their WHOIS Records

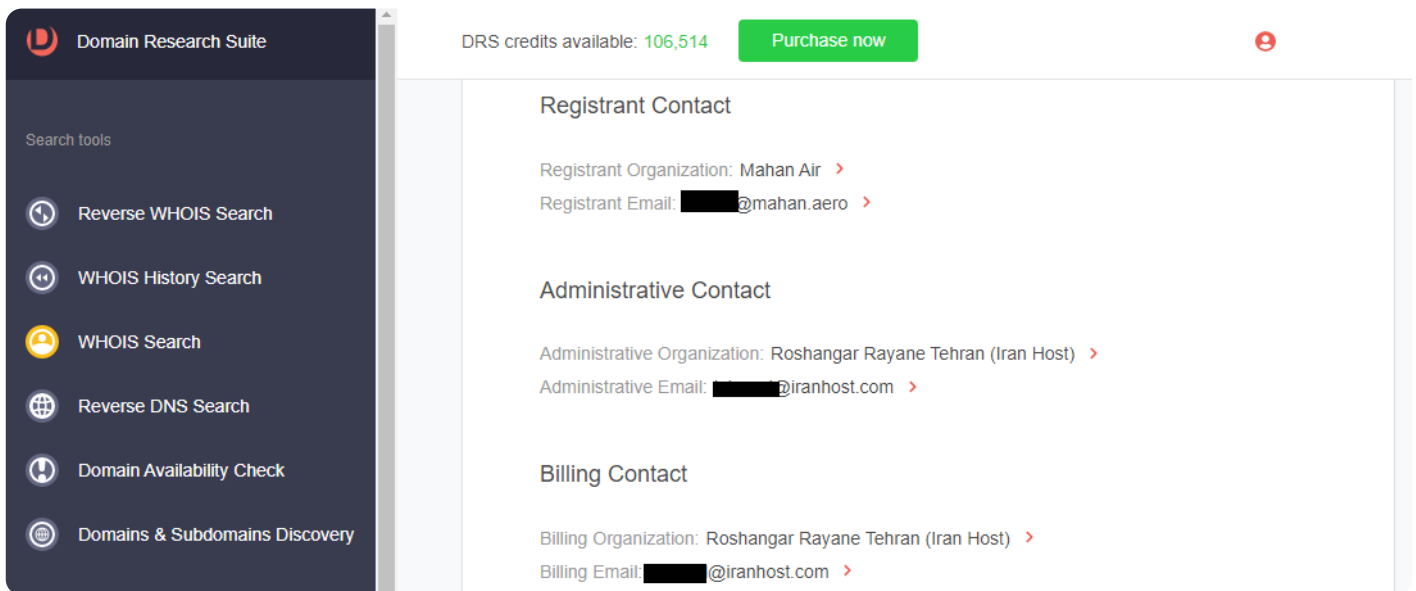
To check who owns particular domains and if they are connected to sanctioned countries, follow these steps:

1. Go to [WHOIS Search](#).
2. Type the domain name into the input field and click **Search**.



The screenshot shows the 'Domain Research Suite' interface. On the left is a dark sidebar with search tools: Reverse WHOIS Search, WHOIS History Search, WHOIS Search (highlighted), and Reverse DNS Search. The main area is titled 'WHOIS Search' and includes a status bar at the top showing 'DRS credits available: 106,514' and a 'Purchase now' button. Below the title, there is a green checkmark icon and the text 'Retrieve domain's actual WHOIS record.' A search input field contains 'khabr-jobs.ir' and is highlighted with a red box. To the right of the input field is a red 'Search' button.

3. Scroll down to the **Registrant Contact** details and copy the registrant organization.

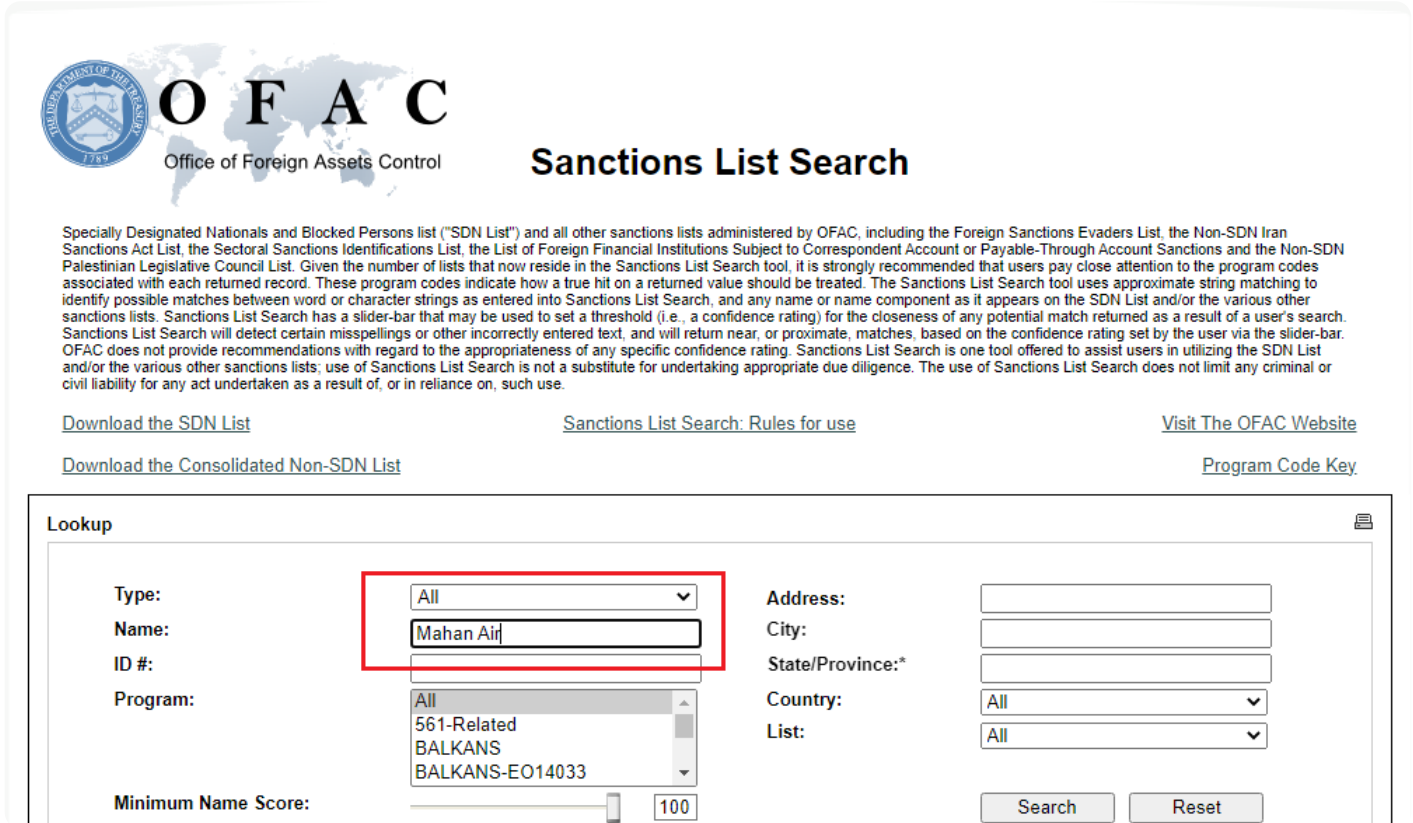


The screenshot shows the 'Registrant Contact' details for the domain 'khabr-jobs.ir'. The interface is the same as the previous screenshot. The 'Registrant Contact' section is expanded, showing the following information:

- Registrant Contact**
  - Registrant Organization: Mahan Air >
  - Registrant Email: [REDACTED]@mahan.aero >
- Administrative Contact**
  - Administrative Organization: Roshangar Rayane Tehran (Iran Host) >
  - Administrative Email: [REDACTED]@iranhost.com >
- Billing Contact**
  - Billing Organization: Roshangar Rayane Tehran (Iran Host) >
  - Billing Email: [REDACTED]@iranhost.com >

4. On another browser tab, go to [OFAC's Sanctions List Search](#).

5. Paste the registrant organization's name into the **Name** field and press Enter.



**OFAC**  
Office of Foreign Assets Control

## Sanctions List Search

Specialy Designated Nationals and Blocked Persons list ("SDN List") and all other sanctions lists administered by OFAC, including the Foreign Sanctions Evaders List, the Non-SDN Iran Sanctions Act List, the Sectoral Sanctions Identifications List, the List of Foreign Financial Institutions Subject to Correspondent Account or Payable-Through Account Sanctions and the Non-SDN Palestinian Legislative Council List. Given the number of lists that now reside in the Sanctions List Search tool, it is strongly recommended that users pay close attention to the program codes associated with each returned record. These program codes indicate how a true hit on a returned value should be treated. The Sanctions List Search tool uses approximate string matching to identify possible matches between word or character strings as entered into Sanctions List Search, and any name or name component as it appears on the SDN List and/or the various other sanctions lists. Sanctions List Search has a slider-bar that may be used to set a threshold (i.e., a confidence rating) for the closeness of any potential match returned as a result of a user's search. Sanctions List Search will detect certain misspellings or other incorrectly entered text, and will return near, or proximate, matches, based on the confidence rating set by the user via the slider-bar. OFAC does not provide recommendations with regard to the appropriateness of any specific confidence rating. Sanctions List Search is one tool offered to assist users in utilizing the SDN List and/or the various other sanctions lists; use of Sanctions List Search is not a substitute for undertaking appropriate due diligence. The use of Sanctions List Search does not limit any criminal or civil liability for any act undertaken as a result of, or in reliance on, such use.

[Download the SDN List](#)      [Sanctions List Search: Rules for use](#)      [Visit The OFAC Website](#)  
[Download the Consolidated Non-SDN List](#)      [Program Code Key](#)

**Lookup**

Type:

Name:

ID #:

Program:   
561-Related  
BALKANS  
BALKANS-EO14033

Minimum Name Score:

Address:

City:

State/Province\*:

Country:

List:

6. Scroll down to see the lookup results. The domain we're investigating, `khabr-jobs[.]ir`, is registered by Mahan Air, which is found on OFAC's sanctions list at the time of this writing.

Lookup

Type:	All	Address:	
Name:	Mahan Air	City:	
ID #:		State/Province*:	
Program:	All 561-Related BALKANS BALKANS-EO14033	Country:	All
Minimum Name Score:	100	List:	All
		Search	Reset

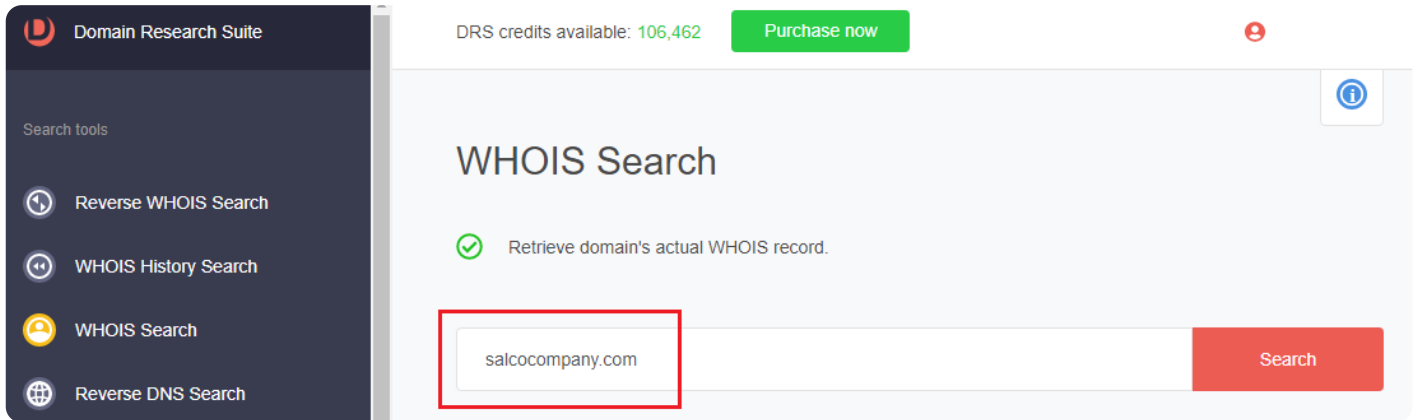
Lookup Results: 2 Found

Name	Address	Type	Program(s)	List	Score
<a href="#">MAHAN AIR</a>	[REDACTED] Fazlollah Exp. Way; First of Karaj High Way	Entity	IFSR; NPWMD; SDGT	SDN	100
<a href="#">MAHAN AIR CO.</a>	[REDACTED] Fazlollah Exp. Way; First of Karaj High Way	Entity	IFSR; NPWMD; SDGT	SDN	100

## Step #2: Find Domains Related to a Sanctioned Entity (with a Specific Website)

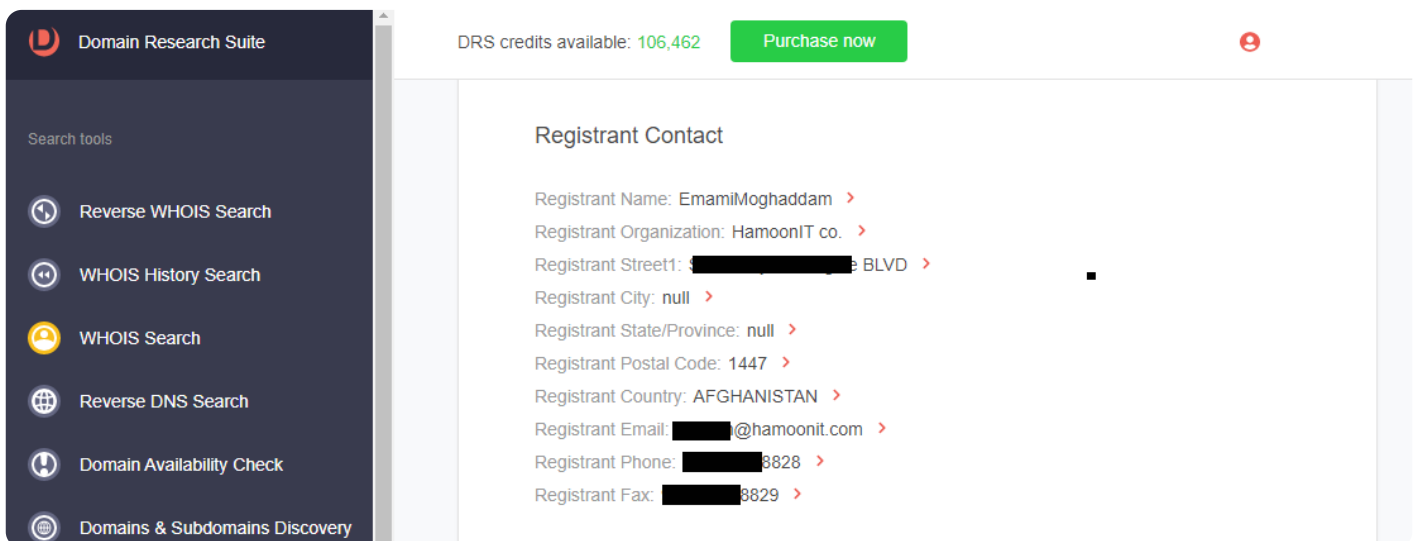
If you need to get a list of domains connected to a sanctioned organization with a website specified by a regulatory entity, follow these steps:

1. Go to [WHOIS Search](#).
2. Type the domain name provided by OFAC. In our demonstration, we used `salcocompany[.]com`, a website associated with South Aluminum Company.



The screenshot shows the 'Domain Research Suite' interface. On the left is a dark sidebar with search tools: Reverse WHOIS Search, WHOIS History Search, WHOIS Search (highlighted), and Reverse DNS Search. The main area is titled 'WHOIS Search' and features a green checkmark icon with the text 'Retrieve domain's actual WHOIS record.' Below this is a search input field containing 'salcocompany.com', which is highlighted with a red box. To the right of the input field is a red 'Search' button. At the top right, there is a green 'Purchase now' button and a notification icon.

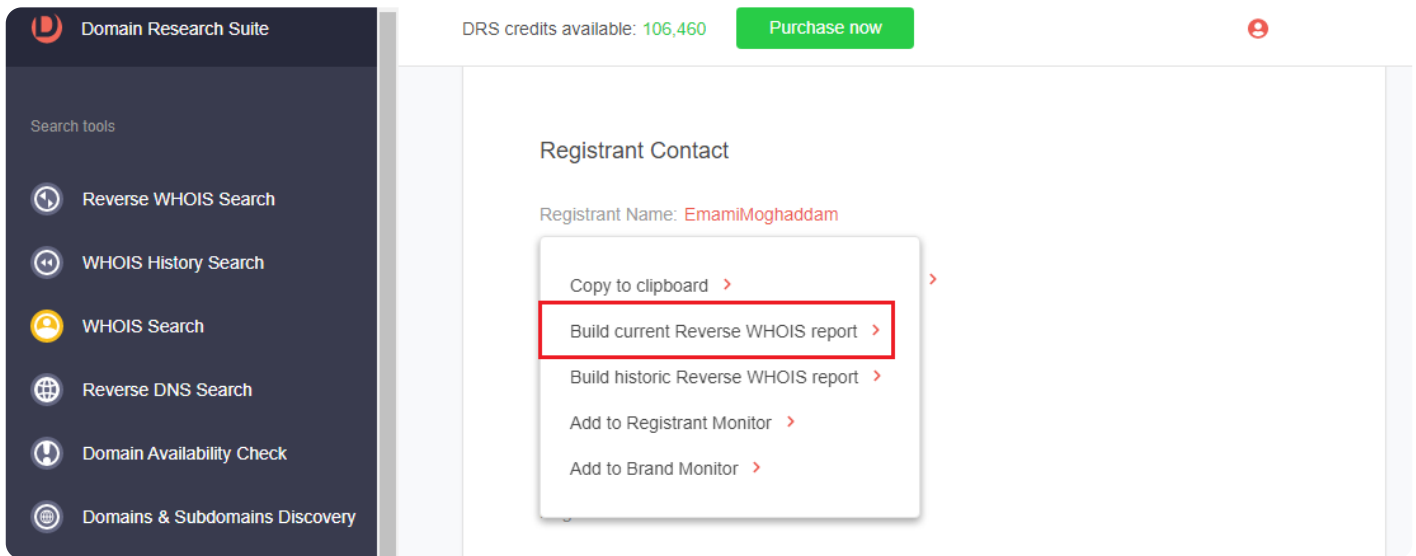
3. Scroll down to the **Registrant Contact** details.



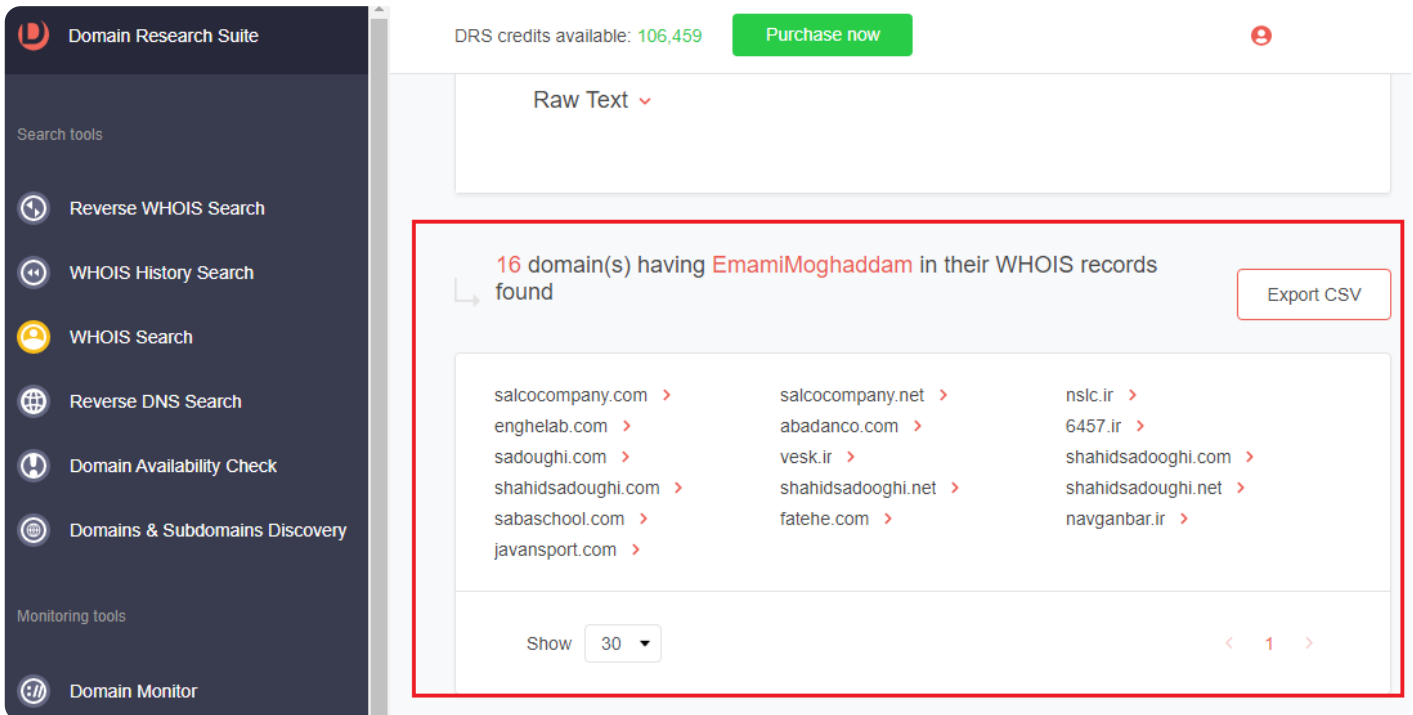
The screenshot shows the 'Registrant Contact' details for the domain. The sidebar on the left now includes 'Domain Availability Check' and 'Domains & Subdomains Discovery'. The main content area displays the following information:

- Registrant Name: EmamiMoghaddam >
- Registrant Organization: HamoonIT co. >
- Registrant Street1: ██████████ BLVD >
- Registrant City: null >
- Registrant State/Province: null >
- Registrant Postal Code: 1447 >
- Registrant Country: AFGHANISTAN >
- Registrant Email: ████████@hamoonit.com >
- Registrant Phone: ████████8828 >
- Registrant Fax: ████████8829 >

4. Click an unredacted registrant data point and pivot off that by selecting **Build current Reverse WHOIS report**.



5. This action will return a list of domains currently registered by the same entity.



The screenshot displays the 'Domain Research Suite' interface. At the top, it shows 'DRS credits available: 106,459' and a 'Purchase now' button. Below this, there's a 'Raw Text' dropdown menu. The main content area is titled '16 domain(s) having EmamiMoghaddam in their WHOIS records found' and includes an 'Export CSV' button. A list of domains is shown, each with a right-pointing arrow:

salccompany.com	salccompany.net	nslc.ir
enghelab.com	abadanco.com	6457.ir
sadoughi.com	vesk.ir	shahidsadooghi.com
shahidsadoughi.com	shahidsadooghi.net	shahidsadoughi.net
sabaschool.com	fatehe.com	navganbar.ir
javansport.com		

At the bottom of the results area, there is a 'Show 30' dropdown menu and pagination controls showing '< 1 >'.

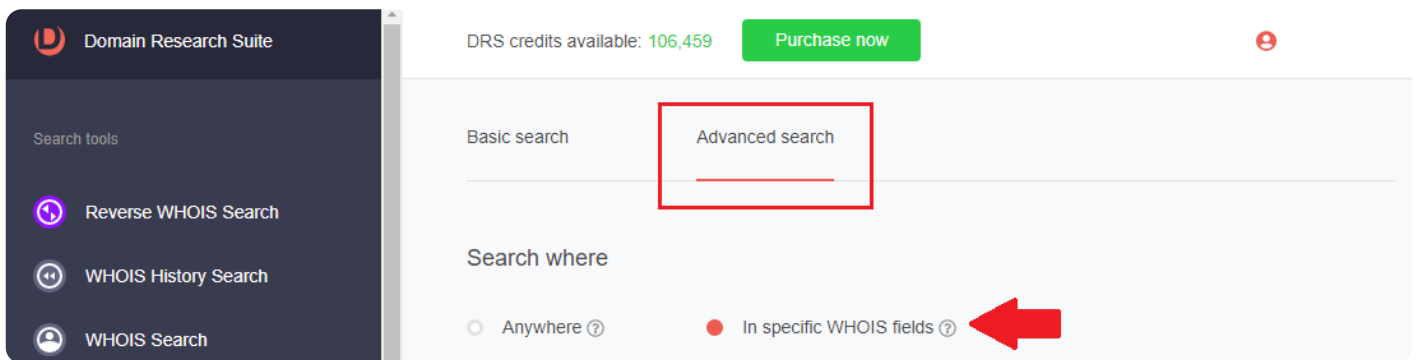
6. **[PRO TIP]:** If the registrant contact details are currently redacted or hidden by WHOIS privacy protection services, use [WHOIS History Search](#) to look for more public records.

## Step #3: Find Domains Related to a Sanctioned Entity (without a Specific Website)

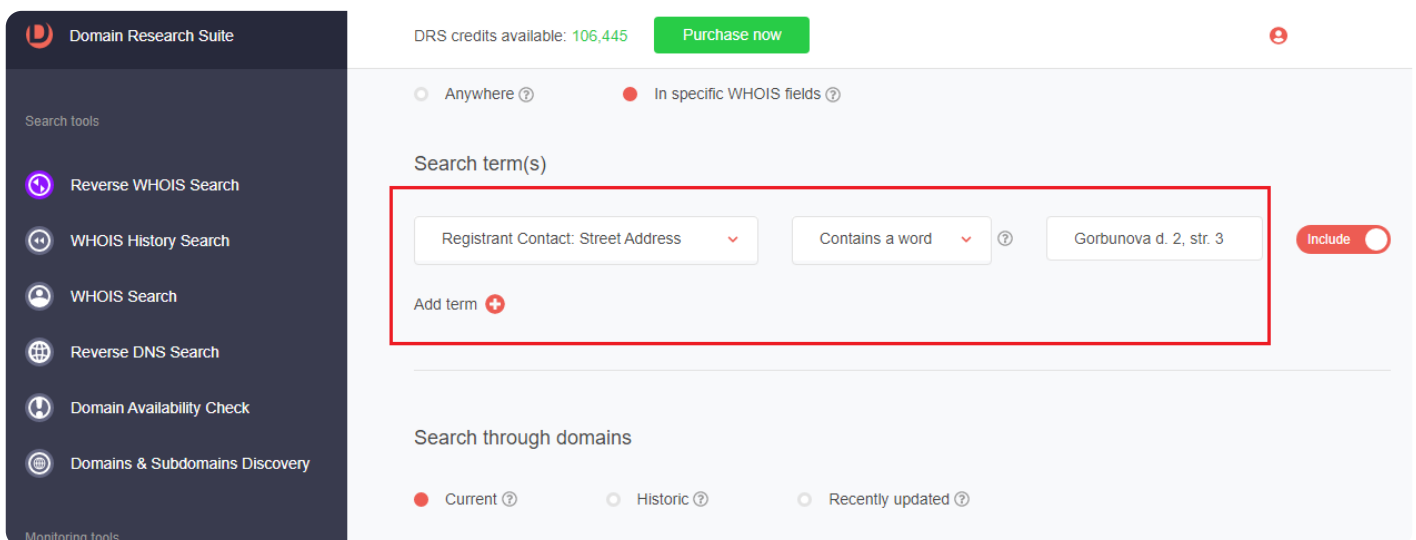
Regulatory entities' listings do not always include a website, so you may only have an address, a phone number, an organization's name, or a person's name on hand. In cases like that, you can still uncover connected domains by following these steps:

1. Go to [Reverse WHOIS Search](#). Go to the **Advanced search** tab and toggle the **In specific WHOIS fields**

radio button on.

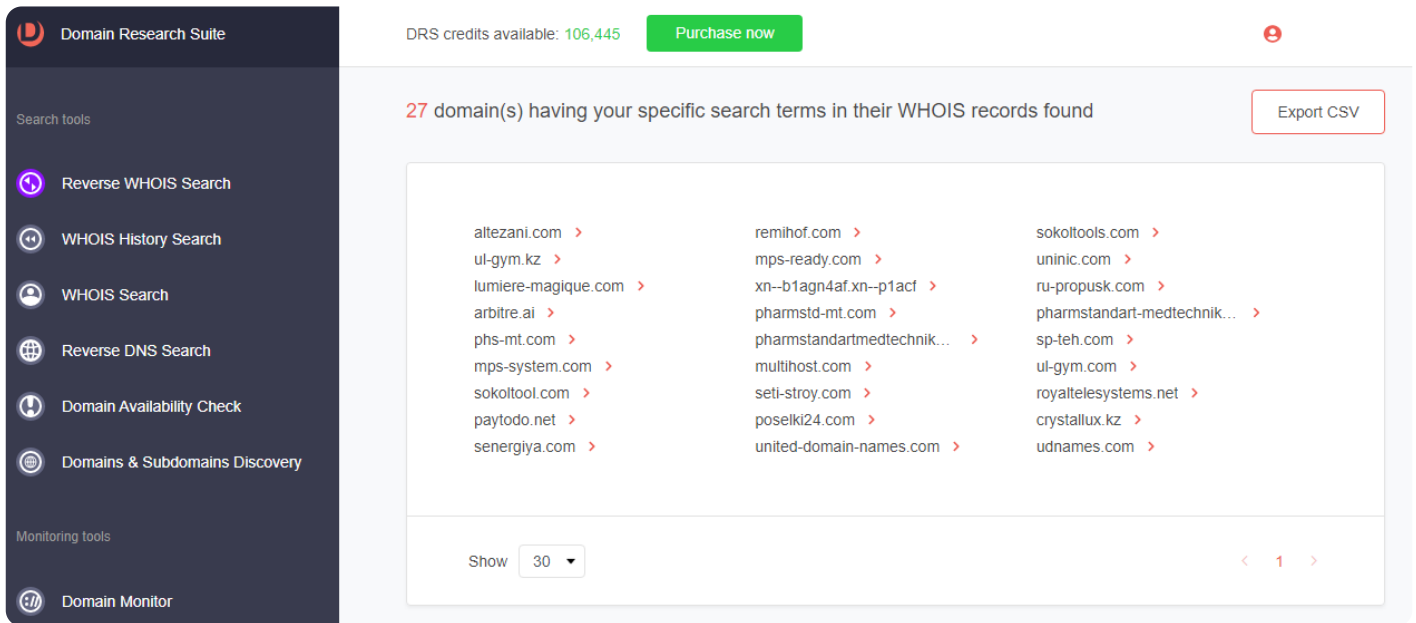


2. Under **Search term(s)**, select the WHOIS record you have available. To illustrate, we looked for domains whose registrant street address matches “Gorbunova d. 2, str. 3,” which is tied to the sanctioned entity Analiticheskii Tsentr Katekhon.





3. Make sure to select **Current** so the results are limited to domains that currently contain the specific WHOIS record detail. For our demonstration, we found 27 domains related to the sanctioned entity.



The screenshot displays the Domain Research Suite (DRS) interface. On the left is a dark sidebar with navigation options under 'Search tools' and 'Monitoring tools'. The main area shows '27 domain(s) having your specific search terms in their WHOIS records found' with an 'Export CSV' button. Below this is a grid of 27 domain names, each with a right-pointing arrow. At the bottom of the grid is a 'Show 30' dropdown and pagination controls.

Search tools	Monitoring tools
Reverse WHOIS Search	Domain Monitor
WHOIS History Search	
WHOIS Search	
Reverse DNS Search	
Domain Availability Check	
Domains & Subdomains Discovery	

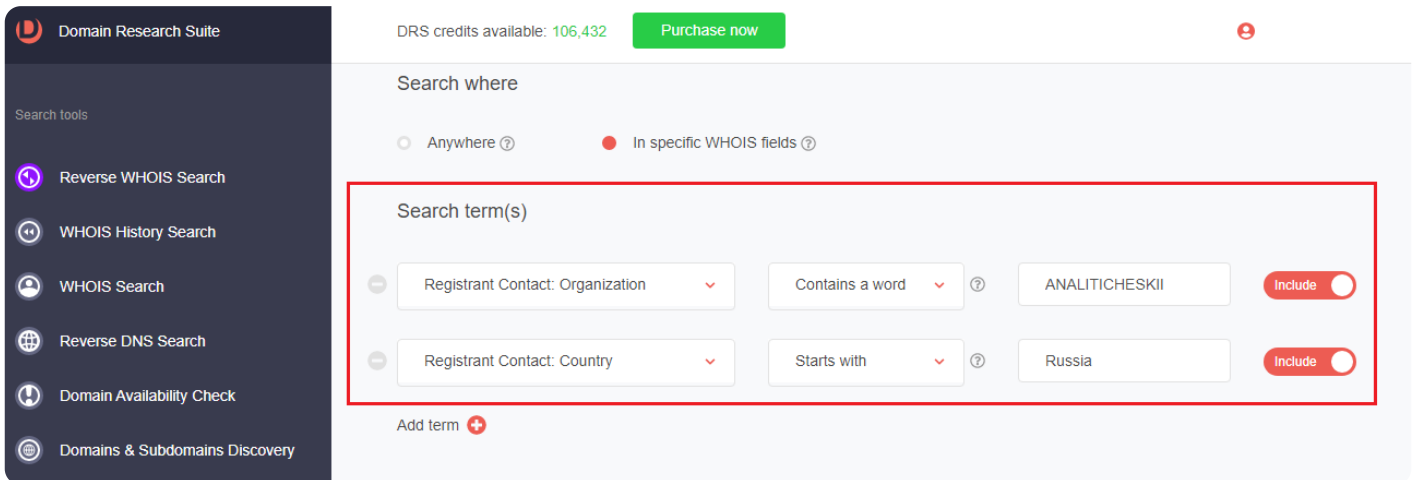
DRS credits available: 106,445 [Purchase now](#)

27 domain(s) having your specific search terms in their WHOIS records found [Export CSV](#)

altezani.com >	remihof.com >	sokoltools.com >
ul-gym.kz >	mps-ready.com >	uninic.com >
lumiere-magique.com >	xn--b1agn4af.xn--p1acf >	ru-propusk.com >
arbitre.ai >	pharmstd-mt.com >	pharmstandart-medtechnik... >
phs-mt.com >	pharmstandartmedtechnik... >	sp-teh.com >
mps-system.com >	multihost.com >	ul-gym.com >
sokoltool.com >	seti-stroy.com >	royaltelesystems.net >
paytodo.net >	poselki24.com >	crystallux.kz >
senergiya.com >	united-domain-names.com >	udnames.com >

Show 30 < 1 >

4. **[PRO TIP]:** You can use other WHOIS data points as search terms. You can also combine multiple WHOIS fields. For example, you can get a list of domains whose registrant organization contains “Analiticheskii Tsentr” and whose registrant country is “Russia.”



Domain Research Suite

DRS credits available: 106,432 [Purchase now](#)

Search where

Anywhere [?](#)  In specific WHOIS fields [?](#)

Search term(s)

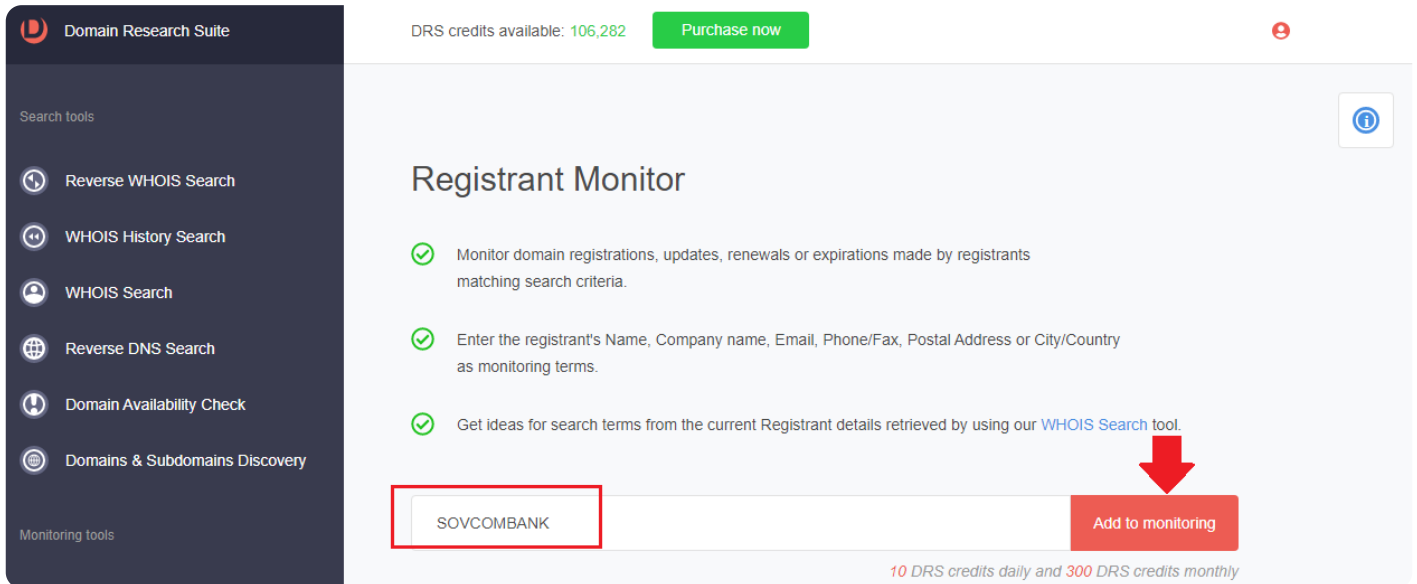
<input type="checkbox"/>	Registrant Contact: Organization	Contains a word	ANALITICHESKII	<input checked="" type="checkbox"/> Include
<input type="checkbox"/>	Registrant Contact: Country	Starts with	Russia	<input checked="" type="checkbox"/> Include

[Add term](#) [+](#)

## Step #4: Monitor the Domain Activities of Sanctioned Entities

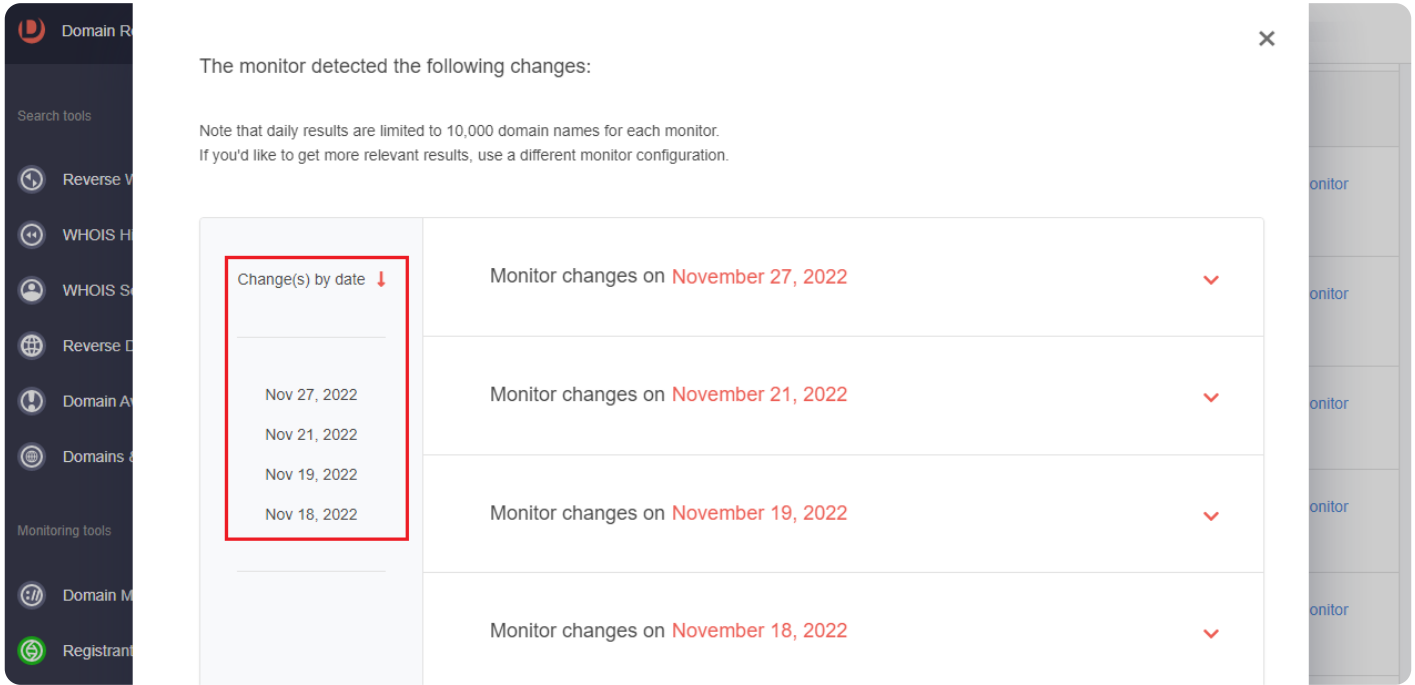
While regulatory entities continue to update its Specially Designated Nationals and Blocked Persons (SDN) list, you may feel the need to keep track of a sanctioned person's or organization's domain activities. Follow these steps to do that:

1. Go to [Registrant Monitor](#).
2. Type the entity name you want to monitor and click **Add to monitoring**. It takes up to 24 hours for the tool to detect newly added, dropped, or updated domains containing the registrant name.



The screenshot shows the 'Registrant Monitor' page in the Domain Research Suite. At the top, it displays 'DRS credits available: 106,282' and a green 'Purchase now' button. The left sidebar lists search tools: Reverse WHOIS Search, WHOIS History Search, WHOIS Search, Reverse DNS Search, Domain Availability Check, and Domains & Subdomains Discovery. The main content area is titled 'Registrant Monitor' and features three bullet points with green checkmarks: 'Monitor domain registrations, updates, renewals or expirations made by registrants matching search criteria.', 'Enter the registrant's Name, Company name, Email, Phone/Fax, Postal Address or City/Country as monitoring terms.', and 'Get ideas for search terms from the current Registrant details retrieved by using our WHOIS Search tool.' Below these points is a search input field containing 'SOVCOMBANK' and a red 'Add to monitoring' button. A red arrow points to the button. At the bottom right, it states '10 DRS credits daily and 300 DRS credits monthly'.

3. Since we started monitoring the entity on 18 November 2022, Registrant Monitor picked up several dropped or updated domains.



The monitor detected the following changes:

Note that daily results are limited to 10,000 domain names for each monitor. If you'd like to get more relevant results, use a different monitor configuration.

Change(s) by date ↓	Monitor changes on	
	November 27, 2022	▼
Nov 27, 2022	November 21, 2022	▼
Nov 21, 2022	November 19, 2022	▼
Nov 19, 2022	November 18, 2022	▼
Nov 18, 2022		

Whether you are interested in investigating sanctioned entities, identifying connected footprints, or keeping tabs on new domain activities, DRS can give you access to the search and monitoring tools you need to conduct a DIY investigation.

***Are you interested in doing a similar investigation to support your regulatory compliance?***

***Access DRS if you are an existing user or [sign up](#) if you are a first-timer.***



WhoisXMLAPI

Perform similar research  
with 500 free DRS credits

**START FREE TRIAL**

(no credit card required)

